CERT Incident Note IN-2000-09: Vulnerability in IRIX telnet daemon

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Systems Compromised Through a Vulnerability in the IRIX telnet daemon

Original release date: Thursday, August 31, 2000
Last revised: Thursday, September 7, 2000
Source: CERT/CC

Overview

We have received reports of intruder activity involving the telnet daemon on SGI machines running the IRIX operating system. Intruders are actively exploiting a vulnerability in *telnetd* that is resulting in a remote root compromise of victim machines.

Information about the vulnerability we have seen exploited as a part of these attacks can be found at

- SGI Security Advisory 20000801-01-P, IRIX telnetd vulnerability
- http://www.securityfocus.com/bid/1572

Description

Reports of successful exploitations of the vulnerability in *telnetd* have included some or all of the following attack characteristics:

- Generation of a syslog message similar to

  ```
  overly long syslog message detected, truncating
  telnetd[xxxxx]: ignored attempt to setenv (_RLD,     ^?D^X^\
  ^?D^X^^   ^D^P^?^?$^B^Cs#^?^B^T#d~^H#e~^P/d~^P/`~^T#`~^O
  ^C ^?^?L/bin/sh
  ```

  or

  ```
  overly long syslog message, integrity compromised, aborting
  ```

- Addition of accounts with root privileges to /etc/passwd
- Remote retrieval and installation of additional intruder tools, including root kits that contain replacements for various system binaries, including *telnetd*
- Installation of packet sniffers
- Installation of irc proxy programs such as *bnc*

Solutions

Patch or disable the telnetd service

Patches for this vulnerability have been released by SGI. Sites are encouraged to follow the instructions outlined in the SGI advisory for specific instructions on how to obtain the patches. For sites that cannot immediately apply the patches, instructions for disabling the telnet service are also provided.

Restrict access to the telnetd service

Sites can employ the use of access control mechanisms, such as packet filtering, firewalls, or application-layer controls to manage the risk of intrusion on vulnerable systems.

As a good security practice in general, the CERT/CC recommends blocking unneeded ports at your network border(s). In particular to this vulnerability, sites should block TCP port 23 (telnet).

For sites which this is not feasible, the CERT/CC recommends applying an access control mechanism such as tcp_wrappers or tcpserver for the telnet service. The tcp_wrappers package can be found at

> ftp://ftp.porcupine.org/pub/security/index.html

The ucspi-tcp package, including tcpserver, can be found at

> http://cr.yp.to/ucspi-tcp.html

If you believe a host has been compromised, we encourage you to disconnect the host from the network and review our steps for recovering from a root compromise:

> http://www.cert.org/tech_tips/root_compromise.html

We also encourage you to ensure that your hosts are current with security patches or work-arounds for well-known vulnerabilities and to regularly review security related patches released by your vendors.

Author: Chad Dougherty

Revision History

```
August 31, 2000: Initial Release
September 7, 2000: Updated information in solutions section upon SGI's release
of patches for this vulnerability, and updated the SGI advisory number.
```