



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

February 12, 2007

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

2007-004

DATE ISSUED:

February 12, 2007

SUBJECT:

Sun Solaris Telnet Remote Authentication Bypass Vulnerability

OVERVIEW:

A vulnerability exists Sun Microsystems Solaris operating system which allows an individual to gain unauthenticated access and would allow an attacker to gain complete control over the affected system. A remote exploit has been published and made available to the general public. At this point in time, a patch is not available although workarounds such as blocking the vulnerable service or implementing a more secure service are recommended.

Affected Systems: Updated

- Solaris 10 x86
- Solaris 10 SPARC

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: **N/A**

DESCRIPTION:

A vulnerability exists in the Telnet daemon (in.telnetd) on Solaris 10 that allows for unauthenticated remote login sessions. The exposure is due to the in.telnetd program sending un-checked, user-supplied information to the login program. A remote attacker who exploits this vulnerability can gain complete control over an affected system. Sun Microsystems does not have any patches available at this time. Organizations affected by this vulnerability are encouraged to implement the recommendations below.

Telnet is an insecure protocol that transmits all authentication and session information in cleartext. Independent of this vulnerability, and in accordance with general security best practices, telnet services should be disabled in favor of a protocol that provides strong encryption and authentication, such as Secure Shell (SSH).

Internet sources have suggested modifying in.telnetd to require "user" authentication mode. Based on testing that we have done, this may break all Telnet connectivity and is not a recommended workaround at this time.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Telnet is an insecure protocol that transmits all authentication and session information in clear text. Independent of this vulnerability, and in accordance with general security best practices, telnet services should be disabled in favor of a protocol that provides strong encryption and authentication, such as Secure Shell (SSH).
- Unless there is a critical business need to do otherwise, Telnet services should be disabled on all hosts.
- If Telnet services are required on a vulnerable system, access from all untrusted hosts and networks should be blocked. By default, Telnet services will run on port 23/TCP. Please be advised that this will not prevent a trusted host from exploiting this vulnerability.

REFERENCES:

US-CERT

<http://www.kb.cert.org/vuls/id/881872>

SANS Internet Storm Center

<http://isc.sans.org/diary.html?storyid=2220>