

# [UNIX] SSLTelnet Daemon Remote Format String Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0028.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/11/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 11 Jul 2004 12:01:56 +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>

-----

SSLTelnet Daemon Remote Format String Vulnerability

---

## SUMMARY

SSLtelnetd is a replacement for telnetd available as part of the FreeBSD <<http://www.freebsd.org/ports/security.html>> ports collection. It implements the Telnet protocol over SSL.

A format string vulnerability exists in SSLTelnet when input is passed to a logging function without proper handling. This could lead to remote code execution.

## DETAILS

Vulnerable Systems:

\* SSLTelnet version 0.13-1

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0640>>  
CAN-2004-0640

The vulnerable piece of code is located in telnetd.c, line 530:

```
SSL_set_verify(ssl_con,ssl_verify_flag,NULL);
```

## Securiteam: [UNIX] SSLTelnet Daemon Remote Format String Vulnerability

```
if (SSL_accept(ssl_con) <= 0) {
    static char errbuf[1024];

    sprintf(errbuf,"SSL_accept error %s\n",
        ERR_error_string(ERR_get_error(),NULL));

    syslog(LOG_WARNING, errbuf); // vulnerable call

    BIO_printf(bio_err,errbuf);

    /* go to sleep to make sure we are noticed */
    sleep(10);
    SSL_free(ssl_con);

    _exit(1);
} else {
    ssl_active_flag=1;
}
```

It can be seen that there is a call to syslog() without proper input validation. The issue can be exploited remotely under certain conditions and would allow remote code execution, usually with root privileges.

### Disclosure Timeline

06/29/2004 Initial vendor contact  
07/02/2004 Secondary vendor contact  
07/08/2004 Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by  
<mailto:idlabs-advisories@idefense.com> iDefense Security.

The original article can be found at:

<<http://idefense.com/application/poi/display?id=114&type=vulnerabilities&flashstatus=true>>  
<http://idefense.com/application/poi/display?id=114&type=vulnerabilities&flashstatus=true>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

### 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.