

[UNIX] tcpflow Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0022.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/03

To: list@securiteam.com

Date: 10 Aug 2003 17:04:58 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

tcpflow Format String Vulnerability

SUMMARY

<<http://www.circlemud.org/~jelson/software/tcpflow/>> tcpflow is a network monitoring tool that records TCP sessions in an easy to use and view manner. This tool contains a format string vulnerability that is typically un-exploitable. However, there have been at least a couple of network management tools (IPNetMonitorX and IPNetSentryX) that allowed this vulnerability to be successfully exploited.

Note: This advisory is being released to inform other developers that may rely on this tool, and to serve as an addendum to the @stake advisory entitled: <<http://www.securiteam.com/securitynews/5EP0G00AUU.html>> "Sustworks Unauthorized Network Monitoring and tcpflow Format String Attack".

DETAILS

tcpflow contains an exploitable format string vulnerability during the opening of a device via libpcap. This code snippet is from the current

Securiteam: [UNIX] tcpflow Format String Vulnerability

version of tcpflow:

From tcpflow:main.c

```
/* make sure we can open the device */
if ((pd = pcap_open_live(device, SNAPLEN, !no_promisc, 1000,
    error)) == NULL)
    die(error);

/* drop root privileges – we don't need them any more */
setuid(getuid());
```

As we can see, if the call to `pcap_open_live()` fails, the error message will be passed to an error handling and cleanup function called `die()`. This happens just before privileges are dropped by the application. Looking at the code snippets below, we can see that this error message will get passed as the format string to the `fprintf()` call inside of `print_debug_message()`. Since the device name is included as part of the libpcap error, and device is specified by the user, an attacker can input format specifiers into `fprintf()`.

From tcpflow:util.c

```
void die(char *fmt, ...)
{
    va_list ap;

    va_start(ap, fmt);
    print_debug_message(fmt, ap);
    exit(1);
}

/*
 * Print a debugging message, given a va_list
 */
void print_debug_message(char *fmt, va_list ap)
{
    /* print debug prefix */
    fprintf(stderr, "%s: ", debug_prefix);

    /* print the var-arg buffer passed to us */
    fprintf(stderr, fmt, ap);

    /* add newline */
    fprintf(stderr, "\n");
    (void) fflush(stderr);
}

```

To test if your version of tcpflow is vulnerable, simply execute tcpflow as root with the command line argument of `-i %x%x%x%x%x%x%x`. If the tcpflow error message contains a large hexadecimal string, your version is vulnerable.

Securiteam: [UNIX] tcpflow Format String Vulnerability

For example:

```
bash-2.05a$ sudo bash
```

```
bash-2.05a# tcpflow -i %x%x%x%x%x%x%x%x
```

```
tcpflow[1195]: BIOCSETIF: 1a45017646365206e1a010365c: Device not  
configured
```

Vendor Response:

There is an updated version of tcpflow available from

<http://www.circlemud.org/~jelson/software/tcpflow>

<http://www.circlemud.org/~jelson/software/tcpflow>.

Recommendation:

Upgrade tcpflow and ensure that it is not setuid root.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

www.atstake.com/research/advisories/2003/a080703-2.txt

www.atstake.com/research/advisories/2003/a080703-2.txt.

The information has been provided by <mailto:daveg@atstake.com> Dave G..

=====

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.