

[UNIX] DSH HOME Environment Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/13/03

To: list@securiteam.com

Date: 13 Aug 2003 12:35:28 +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>

DSH HOME Environment Buffer Overflow

SUMMARY

The <<http://www.netfort.gr.jp/~dancer/software/dsh.html>> DSH package has been found to contain a buffer overflow in the HOME environment variable. This vulnerability will allow attackers to cause the product crash.

DETAILS

Vulnerable systems:

* DSH version 0.24.0

Vulnerable code:

Inside dsh.c:

```
main(int ac, char ** av)
{
    char *buf=NULL;

    setlocale (LC_ALL, "");
```

Securiteam: [UNIX] DSH HOME Environment Buffer Overflow

```
if (!textdomain(PACKAGE_NAME))
{
    if (!bindtextdomain(PACKAGE_NAME, LOCALEDIR))
    fprintf(stderr, "%s: failed to call bindtextdomain\n", PACKAGE);
}
```

```
load_configfile(DSH_CONF);
if (asprintf (&buf, "%s/.dsh/dsh.conf", getenv("HOME")) <
0).....lol
{
    fprintf(stderr, _("%s: asprintf failed\n"), PACKAGE);
    exit (1);
}
load_configfile(buf);
free (buf);
```

asprintfµÄ"Öå£°

```
nt asprintf(char **strp, const char *fmt, ...)
{
    ssize_t buflen = 50 * strlen(fmt); /* pick a number, any number
*/.....lol
    *strp = malloc(buflen);

    if (*strp)
    {
        va_list ap;
        va_start(ap, fmt);
        vsnprintf(*strp, buflen, fmt,
ap);.....lol
        va_end(ap);
        return buflen;
    }
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jsk@ph4nt0m.net>> jsk.

=====

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

=====
=====

Securiteam: [UNIX] DSH HOME Environment Buffer Overflow

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.