

[UNIX] Remote Overflow in tHTTPd (< > replacing)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0115.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/28/03

To: list@securiteam.com

Date: 28 Oct 2003 10:41:35 +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>

Remote Overflow in tHTTPd (< > replacing)

SUMMARY

A vulneability in tHTTPd allows remote attackers to overflow an internal buffer and partially overwrite EBP register and execute arbitrary code.

DETAILS

Vulnerable systems:

- * tHTTPd version 2.21 up to version 2.23b1

Immune systems:

- * tHTTPd version 2.24

The problem is found in libhttpd.c in the function defang()

```
static void defang( char* str, char* dfstr, int dfsz )
```

```
{
    char* cp1;
    char* cp2;

    for ( cp1 = str, cp2 = dfstr;
          *cp1 != '\0' && cp2 - dfstr < dfsz - 1;
          ++cp1, ++cp2 )
    {
```

Securiteam: [UNIX] Remote Overflow in tHTTPd (< > replacing)

```
switch ( *cp1 )
{
  case '<':
    *cp2++ = '&';
    *cp2++ = 'l';
    *cp2++ = 't';
    *cp2 = ';';
    break;
  case '>':
    *cp2++ = '&';
    *cp2++ = 'g';
    *cp2++ = 't';
    *cp2 = ';';
    break;
  default:
    *cp2 = *cp1;
    break;
}
}
*cp2 = '\0';
}
```

So when '<' or '>' are found in the input we "pay for 1 and get 3 for free", this allows us overwrite bits of EBP and indirectly control EIP (assuming its been compiled with gcc < 3.0).

Workaround:
Upgrade to version 2.24

Disclosure Timeline:
09/08/2003: Vendor notified by e-mail
09/12/2003: Vendor replies with working fix
10/27/2003: Public release

ADDITIONAL INFORMATION

The information has been provided by <mailto:advisories@texonet.com>
texonet.com.

=====

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.

Securiteam: [UNIX] Remote Overflow in tHTTPd (< > replacing)

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