

[NEWS] hpaftpd Multiple Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00052.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 26 Mar 2007 13:41:19 +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>

hpaftpd Multiple Buffer Overflows

SUMMARY

<<http://hpaftpd.sourceforge.net/>> hpaftpd is "a high performance anonymous FTP server (RFC 0959). It is designed to run without forks or threads and with low memory usage, so it's suitable for heavy network traffic with very many connections". beSTORM found multiple buffer overflows in hpaftpd, these vulnerabilities are caused by improper usage of the insecure sprintf function.

DETAILS

Vulnerable Systems:
* hpaftpd version 1.01

The hpaftpd reads receives user provided data using the following code:
n = nb_get(nbc, buf, BUF_SIZE - 1);

While BUF_SIZE is defined as:
#define BUF_SIZE 8192

The same BUF_SIZE is used whenever hpaftpd wants to write something to the log/user, here is one example which is returned once the user has provided

[NEWS] hpaftpd Multiple Buffer Overflows

a username:

```
sprintf(obuf, "331 Password required for %s\r\n", ftpc->user);
```

As you can see, even though ftpc->user is limited to 8192, the obuf is also limited to 8192:

```
char buf[BUF_SIZE], obuf[BUF_SIZE]; /* Input buffer, output buffer */
```

Allowing us to supply numerous commands and arguments which in turn will overflow the obuf buffer.

The following commands can be used to overflow the obuf buffer:

- * USER
- * PASS (with a combination of a USER command)
- * CWD
- * MKD
- * RMD
- * DELE
- * RNFR
- * RNTD (with a valid RNFR combination)

Site note:

There appears to be a past attempt to prevent buffer overflows found in the path related functions, as they use snprintf instead of sprintf.

ADDITIONAL INFORMATION

This vulnerability has been found by

<<http://www.beyondsecurity.com/beSTORM>> beSTORM. Visit our web site to download a free 30 day evaluation of beSTORM.

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

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.