

[UNIX] QPopper Buffer Overflow Vulnerability (BULLDIR)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0001.html>

From: support@securiteam.com

Date: 05/01/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 1 May 2002 08:34:32 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

QPopper Buffer Overflow Vulnerability (BULLDIR)

SUMMARY

<<http://www.eudora.com/qpopper/>> QPopper is the most widely used POP3 server for Unix/Linux now includes TLS/SSL. The product has been found to contain a buffer overflow in the way it processes incoming user options.

DETAILS

Vulnerable systems:

* QPopper versions 4.0.3 and 4.0.4

Vulnerable code:

```
pop_bull.c
int CopyOneBull ( POP *p, long bnum, char *name )
{
    FILE *bull;
    char buffer [ MAXMSGLINELEN ];
    BOOL in_header = TRUE;
    BOOL first_line = TRUE;
    int nchar;
    int msg_num;
    int msg_vis_num = 0;
```

Securiteam: [UNIX] QPopper Buffer Overflow Vulnerability (BULLDIR)

```
int msg_ends_in_nl = 0;
char bullName [ 256 ];
MsgInfoList *mp; /* Pointer to message info list */
```

=====

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.



- **Previous message:** support@securiteam.com: "[NEWS] SAP R/3 with Oracle Default Installation Vulnerability"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)