

# [UNIX] libremail Format String (DEBUG, pop.c)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00088.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 26 Dec 2005 18:45:19 +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>

-----

libremail Format String (DEBUG, pop.c)

---

## SUMMARY

<<http://libremail.tuxfamily.org/>> libremail is "a set of command line mail tools, it includes several clients, and allows to filter mails".

A format string vulnerability has been found in libremail's POP handling routines when the library has been set to run in DEBUG mode, the vulnerability can be exploited by remote attackers to cause the library to execute arbitrary code.

## DETAILS

Vulnerable Systems:

\* libremail version 1.1.0 and prior

There is a format string vulnerability in pop.c:

Vulnerable code:

```
[...]  
void lire_pop ()  
{  
int posbuf;
```

## [UNIX] libremail Format String (DEBUG, pop.c)

```
// initialisation
posbuf = 0;

// lecture jusqu'en fin de ligne ou de buffer
do
recv (sockfd, buf_lect + posbuf, 1, 0);
while (buf_lect [posbuf++] != 'n' && posbuf < sz_buflect);

// terminer la chaine de caract res lue (on supprime rn)
if (posbuf > 1 && buf_lect [posbuf - 2] == 'r')
buf_lect [posbuf - 2] = '\0';

else
buf_lect [posbuf - 1] = '\0';

#ifdef DEBUG
putchar ('<');
printf (buf_lect);
#endif
}
```

It could be exploited by tricking a user into connecting to a malicious POP server, or by sending a malicious mail (if the user reads it through a POP server), however it requires that debug mode is activated (not default setting).

### Vendor Status:

The vendor has published updated sources:

<<http://libremail.tuxfamily.org/en/dersources.htm>>  
<http://libremail.tuxfamily.org/en/dersources.htm>

### ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.zone-h.org/en/advisories/read/id=8527/>>  
<http://www.zone-h.org/en/advisories/read/id=8527/>

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

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.

---

- Prev by Date: [\*\[UNIX\] Linux procfs Information Disclosure\*](#)
- Next by Date: [\*\[NT\] dtSearch DUNZIP32.dll Buffer Overflow\*](#)
- Previous by thread: [\*\[UNIX\] Linux procfs Information Disclosure\*](#)
- Next by thread: [\*\[NT\] dtSearch DUNZIP32.dll Buffer Overflow\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)