

# [UNIX] Cyrus IMAP Server Multiple Remote Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0087.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 11/23/04

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

Date: 23 Nov 2004 18:13:10 +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>

-----

Cyrus IMAP Server Multiple Remote Vulnerabilities

---

## SUMMARY

" <<http://asg.web.cmu.edu/cyrus/imapd/>> The Cyrus IMAP server differs from other IMAP server implementations in that it is generally intended to be run on sealed servers, where normal users are not permitted to log in. The mailbox database is stored in parts of the file system that are private to the Cyrus IMAP system. All user access to mail is through the IMAP, POP3, or KPOP protocols. The private mailbox database design gives the server large advantages in efficiency, scalability, and administratively. Multiple concurrent read/write connections to the same mailbox are permitted. The server supports access control lists on mailboxes and storage quotas on mailbox hierarchies."

During an audit of `imapd` several vulnerabilities were discovered ranging from a standard stack overflow, over out of bounds heap corruptions, to a bug caused by the use of programming constructs that are undefined according to the C standard. The bugs may lead to remote server compromise and code execution.

## DETAILS

## Securiteam: [UNIX] Cyrus IMAP Server Multiple Remote Vulnerabilities

### Vulnerable Systems:

- \* Cyrus IMAP Server versions 2.2.8 and prior

### Immune Systems:

- \* Cyrus IMAP Server versions 2.2.9

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1011>>

CAN-2004-1011 – IMAPMAGICPLUS preauthentication overflow

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1012>>

CAN-2004-1012 – PARTIAL command out of bounds memory corruption

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1013>>

CAN-2004-1013 – FETCH command out of bounds memory corruption

### IMAPMAGICPLUS preauthentication overflow

When the option `imapmagicplus` is activated on a server the `PROXY` and `LOGIN` commands suffer a standard stack overflow, because the username is not checked against a maximum length when it is copied into a temporary stack buffer. This bug is especially dangerous because it can be triggered before any kind of authentication takes place.

Note: Affected Cyrus IMAP versions: 2.2.4 to 2.2.8 inclusive.

### PARTIAL command out of bounds memory corruption

Due to a bug within the argument parser of the `partial` command an argument like `"body[p]"` will be wrongly detected as `"body.peek"`. Because of this the `bufferposition` gets increased by 10 instead of 5 and could therefore point outside the allocated memory buffer for the rest of the parsing process. In `imapd` versions prior to 2.2.7 the handling of `"body"` or `"bodypeek"` arguments was broken so that the terminating `']'` got overwritten by a `'\0'`. Combined the two problems allow a potential attacker to overwrite a single byte of `malloc()` control structures, which leads to remote code execution if the attacker successfully controls the heap layout.

Note: Affected Cyrus IMAP versions: 2.2.6 and prior.

### FETCH command out of bounds memory corruption

The argument parser of the `fetch` command suffers a bug very similar to the `partial` command problem. Arguments like `"body[p]"`, `"binary[p]"` or `"binary[p]"` will be wrongly detected and the buffer position can point outside of the allocated buffer for the rest of the parsing process. When the parser triggers the `PARSE_PARTIAL` macro after such a malformed argument was received this can lead to a similar one byte memory corruption and allows remote code execution, when the heap layout was successfully controlled by the attacker.

Note: Affected Cyrus IMAP versions: 2.2.8 and prior.

### APPEND command uses undefined programming construct

To support `MULTIAPPENDS` the `cmd_append` handler uses the global `stage` array. This array is one of the things that gets destructed when the

## Securiteam: [UNIX] Cyrus IMAP Server Multiple Remote Vulnerabilities

fatal() function is triggered. When the Cyrus IMAP code adds new entries to this array this is done with the help of the postfix increment operator in combination with memory allocation functions. The increment is performed on a global variable counting the number of allocated stages. Because the memory allocation function can fail and therefore internally call fatal() this construct is undefined according to ANSI C.

This means that it is not clearly defined if the 'numstage' counter is already increased when fatal() is called or not. While older GCC versions increase the counter after the memory allocation function has returned, newer GCC versions (3.x) increase the counter value prior to that. In such a case the stage destruction process will try to free an uninitialized and maybe attacker supplied pointer. Again this could lead to remote code execution. Because it is hard for an attacker to let the memory allocation functions fail in the right moment.

### Vendor Status:

The developers of Cyrus IMAP have already released a new version for the IMAP server. Users are highly encouraged to upgrade to the newer 2.2.9 version.

### Disclosure Timeline:

- 06. November 2004 – Sent an email to the Cyrus IMAP team
- 11. November 2004 – Got reply from the Cyrus developers and shared the information with vendor-sec
- 17. November 2004 – Cyrus IMAP team contacted vendor-sec with the official patch
- 22. November 2004 – Cyrus IMAP Server 2.2.9 released
- 22. November 2004 – Public Disclosure

### ADDITIONAL INFORMATION

The information has been provided by <mailto:s.esser@e-matters.de> Stefan Esser.

The original article can be found at:

<<http://security.e-matters.de/advisories/152004.html>>  
<http://security.e-matters.de/advisories/152004.html>

=====

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,

Securiteam: [UNIX] Cyrus IMAP Server Multiple Remote Vulnerabilities

loss of business profits or special damages.