

# [UNIX] Fetchmail DoS and Code Execution Vulnerabilities (POP3, UID)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0033.html>

---

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

*Date:* 08/08/05

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

Date: 8 Aug 2005 15:38:03 +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>

-----

Fetchmail DoS and Code Execution Vulnerabilities (POP3, UID)

---

## SUMMARY

fetchmail is "a software package to retrieve mail from remote POP2, POP3, IMAP, ETRN or ODMR servers and forward it to local SMTP, LMTP servers or message delivery agents".

The POP3 code in fetchmail-6.2.5 and older that deals with UIDs (from the UIDL) reads the responses returned by the POP3 server into fixed-size buffers allocated on the stack, without limiting the input length to the buffer size. A compromised or malicious POP3 server can thus overrun fetchmail's stack. This affects POP3 and all of its variants, for instance but not limited to APOP.

In fetchmail-6.2.5.1, the attempted fix prevented code injection via POP3 UIDL, but introduced two possible NULL dereferences that can be exploited to mount a denial of service attack.

## DETAILS

Vulnerable Systems:

\* fetchmail version 6.2.5.1 (denial of service)

## Securiteam: [UNIX] Fetchmail DoS and Code Execution Vulnerabilities (POP3, UID)

- \* fetchmail version 6.2.5 (code injection)
- \* fetchmail version 6.2.0 (code injection)

### Immune Systems:

- \* fetchmail version 6.2.5.2
- \* fetchmail version 6.2.6-pre7
- \* fetchmail version 6.3.0 (not released yet)

### Impact:

In fetchmail-6.2.5 and older, very long UIDs can cause fetchmail to crash, or potentially make it execute code placed on the stack. In some configurations, fetchmail is run by the root user to download mail for multiple accounts.

In fetchmail-6.2.5.1, a server that responds with UID lines containing only the article number but no UID (in violation of RFC-1939), or a message without Message-ID when no UIDL support is available, can crash fetchmail.

### Solution:

Upgrade your fetchmail package to version 6.2.5.2.

You can either download a complete tarball of fetchmail-6.2.5.2.tar.gz, or you can download a patch against fetchmail-6.2.5 if you already have the 6.2.5 tarball. Either is available from:

<[http://developer.berlios.de/project/showfiles.php?group\\_id=1824](http://developer.berlios.de/project/showfiles.php?group_id=1824)>  
[http://developer.berlios.de/project/showfiles.php?group\\_id=1824](http://developer.berlios.de/project/showfiles.php?group_id=1824)

### To use the patch:

1. download fetchmail-6.2.5.tar.gz (or retrieve the version you already had downloaded) and fetchmail-patch-6.2.5.2.tar.gz
2. unpack the tarball: `gunzip -c fetchmail-6.2.5.tar.gz | tar xf -`
3. unpack the patch: `gunzip fetchmail-patch-6.2.5.2.gz`
4. apply the patch: `cd fetchmail-6.2.5 ; patch -p1 <../fetchmail-patch-6.2.5.2`
5. now configure and build as usual - detailed instructions in the file named "INSTALL".

### ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:ma+nomail@dt.e-technik.uni-dortmund.de>> Matthias Andree.

The original article can be found at:

<<http://fetchmail.berlios.de/fetchmail-SA-2005-01.txt>>  
<http://fetchmail.berlios.de/fetchmail-SA-2005-01.txt>

=====

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)

Securiteam: [UNIX] Fetchmail DoS and Code Execution Vulnerabilities (POP3, UID)

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.