

# [UNIX] Multiple Security Vulnerabilities in W3Mail

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0037.html>

---

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

*Date:* 11/14/02

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

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

Date: 14 Nov 2002 17:33:30 +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)

-----

Multiple Security Vulnerabilities in W3Mail

---

## SUMMARY

<<http://www.cascadesoft.com/>> W3Mail is the perfect choice if you are seeking a low cost webmail solution that will keep your IT department headache free, and provide your email users with the tools they need to use email from the road.

This vulnerability comes in 3 related parts.

On 1.0.5 and earlier releases:

1) W3Mail can incorrectly expose downloaded MIME attachments without correct authentication in cases where the web server has been configured with indexing for the MIME attachments storage directory.

2) In cases where the web server has server side scripting of any type (such as PHP) enabled for the MIME attachments directory, it is possible to gain remote access as the web server user typically nobody.

On 1.0.6:

3) W3Mail can be made to retrieve any file to which the web server user has read access (for example /etc/passwd).

## DETAILS

## Securiteam: [UNIX] Multiple Security Vulnerabilities in W3Mail

Technical details:

On 1.0.5 and earlier releases:

1) Unless indexing for the MIME attachments directory is disabled it is possible to browse the MIME attachments directory and read arbitrary attachments. Prior to release 1.0.3, W3Mail did not correctly clean up the MIME directory, leaving the attachments there even after the user whom they belonged to has logged out. In releases 1.0.3 and onwards, providing the user correctly logs out their attachments will be removed. Note that the attachments will remain as with 1.0.3 and previous releases if the user simply closes the window rather than using the correct logout link.

2) By sending a MIME attachment executable by the web server from the MIME attachments directory to an POP3 account accessed from the W3Mail web based POP3 client remote access as the web server user can in theory be achieved, if the user to whom the mail is sent opens the malicious email (and thus creates the attachments within the MIME attachments directory for the lifetime explained in part 1). Whilst the attachment exists, the potential intruder can request it via their browser and therefore have it expected by the web server. The attachment must be sent as a none text MIME type in order for the malicious code to correctly be created. This part of the vulnerability will work even when directory indexing is turned off for the MIME attachments directory since attachments are created with their original name.

This vulnerability can also be exploited on attachments being sent from W3Mail, although in this case the affect is reduced in releases from 1.0.3 onwards which clean the attachments directory after the mail has been sent minimizing the potential time for any attack.

On 1.0.6:

3) In replacing the code to fix the problems described previously, CascadeSoft moved the MIME attachments directory out of the document root as we initially recommended. However, the code they introduced to allow access to the attachments from the web page (viewAttachment.cgi) can be made to read any arbitrary file that the web server user has read access to, as it makes no sanity checks on the value passed within the file element of the URL, allowing for file=../../../../etc/passwd etc. Note that for this to work as described the attacker will need a valid session ID.

Solutions:

In order to completely protect against the vulnerability (in the short term), Nth Dimension recommend turning off indexing and any server side file execution for the MIME attachments directory, however it is our belief that it would be better to rewrite the affected code with a view to storing attachments (either those being sent or received) outside the web servers document root. Release 1.0.6 fixes issues 1 & 2 as Tim Brown suggested but introduces a new hole which allows retrieval of arbitrary files using the new readAttachment.cgi script. It may be mitigated by the following (untested) patch:

## Securiteam: [UNIX] Multiple Security Vulnerabilities in W3Mail

8a9

> *use File::Basename;*

18c19

< \$file = \$form->param('file');

- ----

> *\$file = basename(\$form->param('file'));*

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[timb@nth-dimension.org.uk](mailto:timb@nth-dimension.org.uk)>  
Tim Brown.

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] Vulnerability Found in Benchmark Tool for HTTP Pages"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)