

Securiteam: [NT] Mailtraq Multiple Vulnerabilities (CSS, Path Disclosure, Source Viewing)

# [NT] Mailtraq Multiple Vulnerabilities (CSS, Path Disclosure, Source Viewing)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0007.html>

---

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

**Date:** 06/09/03

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

Date: 9 Jun 2003 17:23:57 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,  
or call 617-399-6980

-----

Mailtraq Multiple Vulnerabilities (CSS, Path Disclosure, Source Viewing)

---

## SUMMARY

Mailtraq is "the alternative to Microsoft Exchange. It is the most powerful email server yet, providing industrial-strength email services for your organization using POP3, SMTP, IMAP, LDAP, and HTTP – compatible with all major email clients. A Windows-based software solution, Mailtraq provides a secure platform, with on-line virus detection integration, spam filtering, web mail, instant messaging and more". The product has been found to contain three security vulnerabilities, one allowing attacker to reveal the true path under which the product has been installed, the other allows sending malicious content via the server (i.e. Cross Site Scripting vulnerability), and another allows viewing the source code of the web applications installed on the server.

## DETAILS

Vulnerable systems:

Securiteam: [NT] Mailtraq Multiple Vulnerabilities (CSS, Path Disclosure, Source Viewing)

\* Mailtraq version 2.3.0.1413

Examples:

Using the following URL <http://10.10.10.1/browse.asp>. will cause the server to return the content of the ASP file.

Using the following URL <http://10.10.10.1/browse.asp>\* will cause the server to return the true path under which the product was installed.

Using the following URL [http://10.10.10.1/browse.asp?cfolder=<script>alert\(document.cookie\)</script>](http://10.10.10.1/browse.asp?cfolder=<script>alert(document.cookie)</script>) will cause the server to return arbitrary JavaScript in the response allowing attacker to initiate a Cross Site Scripting vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <mailto:vulncode@yahoo.com> Ziv Kamir.

=====

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, loss of business profits or special damages.