

# [NT] Eudora Script Execution Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0059.html>

---

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

*Date:* 11/21/02

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

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

Date: 21 Nov 2002 11:17:45 +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)

-----

Eudora Script Execution Vulnerability

---

## SUMMARY

<<http://www.eudora.com>> Qualcomm Inc.'s Eudora is a graphical e-mail client for Windows and Macintosh. A vulnerability in the product allows remote attackers to cause the product to execute arbitrary script codes.

## DETAILS

Remote exploitation of a weakness in Eudora could allow for the potential retrieval of sensitive information from a targeted Eudora user's computer.

Eudora saves e-mail attachments in a predictable location. Exploitation works as such: an attacker sends an e-mail to a Eudora user that directs him to a specific URL; the e-mail also contains an HTML-enabled e-mail attachment that contains scripting code. If the user is socially engineered into clicking on the link, then a frames page can load the attachment in one of its frames. The attachment can then retrieve (within the security settings of the local zone) the content of any local file, and transmit it back to the attacker. The attack script, in turn, can retrieve the contents of any local file and transmit it back to the attacker. Since the issue is simple to exploit, and the issue has still not been addressed, a sample attack script is not included in this advisory.

## Securiteam: [NT] Eudora Script Execution Vulnerability

### Analysis:

Exploitation could lead to further compromise if the attacker is able to retrieve sensitive files such as the Windows SAM table. It is also possible for the attacker to obtain other confidential information. A secure implementation would involve using a random string within the directory structure to prevent this class of attacks (e.g. Mozilla e-mail client, etc.).

### Detection:

Eudora 5.1.1 and 5.2 are confirmed to be vulnerable; other versions may be affected as well.

To determine susceptibility, send an e-mail with an attachment to a test Eudora user. Check if Eudora stores it in the C:\Program Files\Qualcomm\Eudora\attach\ directory (assuming a default installation).

### Workaround:

Change the default location where Eudora stores e-mail attachments.

### Vendor response:

A Eudora Tech Support Specialist provided the following response (from head Eudora developer):

"In rare circumstances, certain ill-formatted MIME boundaries can cause Eudora to crash. It is exceedingly unlikely that this problem could be exploited to undermine security. The problem will be fixed in the next release of Eudora."

[iDEFENSE note: The response does not address the security implications of this advisory. Two attempts were made to change or clarify Qualcomm's response; all to no avail.]

### Disclosure timeline:

09/12/2002 Issue disclosed to iDEFENSE

10/14/2002 Qualcomm notified ([eudora-custserv@eudora.com](mailto:eudora-custserv@eudora.com))

10/14/2002 iDEFENSE clients notified

10/15/2002 Auto-response received

10/31/2002 Second attempt at contact

11/07/2002 Third attempt at contact

11/08/2002 Vendor response from J. Michael L. ([mlreply@qualcomm.com](mailto:mlreply@qualcomm.com))

11/10/2002 Clarification request of Vendor Response from iDEFENSE

11/11/2002 Same response from J. Michael L. ([mlreply@qualcomm.com](mailto:mlreply@qualcomm.com))

11/12/2002 Second clarification request of Vendor Response from iDEFENSE

11/19/2002 Still no reply for vendor clarification of response

11/19/2002 Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:dendler@idefense.com>> David Endler of iDEFENSE, the vulnerability was discovered by <<mailto:bennett@peacefire.org>> Bennett Haselton.

Securiteam: [NT] Eudora Script Execution Vulnerability

=====

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.