

[NT] Eudora 5.x for Windows Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0023.html>

From: support@securiteam.com

Date: 08/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 8 Aug 2002 10:52:36 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Eudora 5.x for Windows Buffer Overflow Vulnerability

SUMMARY

<<http://www.qualcomm.com/>> Eudora developed and distributed by QUALCOMM Inc. is a Mail User Agent running on Windows 95/98/2000/ME/NT 4.0 and MacOS 8.1 or later. Eudora 5.x for Windows contains a buffer overflow vulnerability, which could allow a remote attacker to execute arbitrary code.

DETAILS

Vulnerable systems:

* Eudora 5.0-J for Windows (Ver.5.0.2-Jr2 trial) [Japanese]

* Eudora 5.1.1 for Windows (Sponsored Mode) [English]

The buffer overflow occurs when Eudora receives a message using 139 bytes or more of string as a boundary, which is used to divide a multi-part message into separate parts. In our verification environment, we have found that this could allow arbitrary commands to be executed.

Solution:

You can limit your exposure to this problem by using content filtering software that screen out email messages using 139 bytes or more of string

Securiteam: [NT] Eudora 5.x for Windows Buffer Overflow Vulnerability

as a boundary.

QUALCOMM Inc. reported that this problem would be fixed in the next release [English].

Livin' on the EDGE Co., Ltd. reported that this problem would be fixed in Eudora5.1-J for Windows [Japanese] of the next release.

Vendor communication:

6 Jun 2002: We discovered the vulnerability.

6 Jun 2002: We reported the findings to win-eudora-bugs@kuni.co.jp

14 Jun 2002: the findings were reported again to win-eudora-bugs@kuni.co.jp

17 Jun 2002: We contacted QUALCOMM Inc. .

18 Jun 2002: QUALCOMM Inc. sent a reply stating that they had started an investigation of the problem.

3 Jul 2002: We asked QUALCOMM Inc. about the progress of the investigation

19 Jul 2002: We asked QUALCOMM Inc. again about the progress of the investigation

24 Jul 2002: We informed QUALCOMM Inc. about the announcement schedule of this advisory

25 Jul 2002: QUALCOMM Inc. reported that this problem would be fixed in the next release

5 Aug 2002: We decided to disclose this vulnerability due to concern over the potential consequences this issue may cause.

win-eudora-bugs@kuni.co.jp has not provided any comments on this issue as of August 5, 2002.

6 Aug 2002: It turns out that connection has not reached Livin' on the EDGE Co., Ltd. (user support of Japanese version). Livin' on the EDGE Co., Ltd. reported that this problem would be fixed in the next release immediately.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:n-miwa@lac.co.jp>> Nobuo Miwa LAC.

=====

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.

- ***Previous message:*** support@securiteam.com: "[NT] Unchecked Buffer in Content Management Server Could Enable Server Compromise"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)