

Re: Eudora MUA: Risky practice

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-08/0386.html>

From: Will Bryant (will@core-dev.co.nz)

Date: 08/27/01

Message-Id: <5.1.0.14.2.20010828033800.03fb0db0@ish.sharechat.co.nz>

Date: Tue, 28 Aug 2001 04:27:39 +1200

To: bugtraq@securityfocus.com

From: Will Bryant <will@core-dev.co.nz>

Subject: Re: Eudora MUA: Risky practice

> A user deleting the attachments from the disk (for example,
> hundreds of
> copies of Sircam) can execute one of them by accident. This deletion is
> usually done from the Windows file manager, which will never ask for
> confirmation before executing a file. [snip]

Note that recent versions of Eudora have a feature to prevent exactly this problem – when opening certain types of files in your attachments directory from Explorer (yes, outside Eudora itself), you will be given a yes/no confirmation prompt with this warning:

'The file "<file name>" may contain programs or macros. Opening it might transmit your data over the Internet, or alter, damage, or remove files and applications on your computer. Unless you not only trusted the sender, but also expected this file, you may not wish to open it. Do you wish to open it?'

Not as perfect solution, but definitely a good idea anyway.

It only happens for certain file types –

HKCR\Software\Qualcomm\Eudora\LaunchManager lists the paths (both the attachments and embedded folders) and file extensions (ade, adp, bas, bat, chm, cmd, com, cpl, crt, do, exe, hlp, ht, inf, ins, isp, js, lnk, md, ms, pcd, pif, pl, pot, pp, pwz, reg, scr, sct, shb, shs, url, vb, ws, xl) it will prompt for. (Incidentally, it doesn't prompt for .url files for me even though they're on the list. Haven't tested all the others.)

I don't know how it's implemented – some sort of shell extension, I assume it just hooks all opens from Explorer and checks them against the lists. Perhaps someone at Qualcomm can fill us in?

Personally I would however still prefer it to not extract attachments out to the directory automatically – it is more manageable than say Outlook Express where people tend to end up with 90mb mail folders, but it does cause a lot of mess and worry for those of us who use Eudora to read

Re: Eudora MUA: Risky practice

SecurityFocus Bugtraq: Re: Eudora MUA: Risky practice

bugtraq :) (and it's a pain when you get a lot of mail with attachments.) IMHO it would be much nicer if it say didn't seperate the attachments by default, but let you do it manually.

Fixing the problem noted on bugtraq a while back where people can 'fake' attachments by putting in the 'Attachment Converted:' text in the body of an email would be good, too.

Will Bryant, will@core-dev.co.nz cell +64 21 655 443
<http://www.core-dev.co.nz/> Personal: <http://carcino.gen.nz/>
[PGP 0x96A7F40A, FP 827F A2A9 C718 106D 8F80 E16E A244 D5F2 96A7 F40A]

- *Previous message:* [Larry W. Cashdollar: "Dangerous temp file creation during installation of Netscape 6."](#)
- *In reply to:* [Borja Marcos: "Eudora MUA: Risky practice"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)