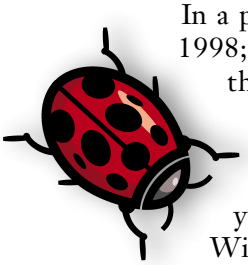
Email bug alert!

On July 27, the Secure Programming Group at Finland's Oulu University discovered a serious security flaw in popular email software of both Microsoft and Netscape.



In a previous column (*CMAJ* 1998;159:173) I mentioned that computer viruses associated with email attachments can infect your computer only if you run the program. With this security flaw, however, the virus is embedded in the name of the email attachment itself. In effect, a prankster can form a file name that is extra long; it forces a "buffer overflow," allowing harmful code embedded in the file name itself to do irreparable harm to your computer. The most important message to remember is that this bug can affect your system even if you do not run the program.

The virus affects Microsoft Outlook 98 on Windows 95, Windows 98, and Windows NT, as well as Outlook Express, which was shipped with Internet Explorer 4.0 and 4.01 on Windows 95, Windows 98, Windows NT 4.0, Windows NT for DEC Alpha, Macintosh and Unix. Windows 3.X and Windows NT 3.51 versions of Internet Explorer are not affected.

Netscape has confirmed that the bug affects the mail and news components of Netscape Communicator 4.0 to 4.05 on Windows 3.1, 95, 98 and NT platforms, and Netscape Communicator 4.5 Preview Release 1 on Windows 95, 98 and NT. It does not affect Macintosh and Unix platforms. Pegasus Mail and Qualcomm's Eudora are not vulnerable to this particular bug.

Computer users should note that this alert only points to a *potential* security threat; as of September, there had been no reports of computers being affected by the bug.

What you can do

At the time of writing, both Microsoft and Netscape have posted patches for this security flaw, and if you are using any of the affected systems, download it immediately. The Microsoft Outlook patch is located at **www.microsoft.com/outlook/default.asp** and the Outlook Express patch is at **www.microsoft.com/ie/**.

Netscape has released Communicator 4.06 that includes a vulnerability fix; this new version may be downloaded at **www.netscape.com**.

Up-to-date security advisories and alerts are available from the Australian Computer Emergency Response Team at **www.auscert.org.au** and the US Computer Emergency Response Team at **www.cert.org**.

Related virus warning

The following message or a variant has recently been circulating via email:

Microsoft Internet Explorer Support Center <IEsupport @microsoft.com> on 08/07/98 03:40:04 PM

To: [Addressee deleted]

Subject: FREE! Your upgrade for Microsoft Internet Explorer

As user of Microsoft Internet Explorer, Microsoft Corporation provide you an upgrade for your Microsoft Internet Explorer. Please run Ie080898.exe to install the upgrade. This file will fix some serious bugs in your Internet Explorer. For more information please visit Microsoft Internet Explorer Home Page at: http://www.microsoft.com/ie/.

If you receive it, **do not run the program, and delete the message immediately**. Microsoft does not distribute upgrades and patches via email.

This message contains a computer virus that has 2 variants: one version deletes all the information on your hard drive, and the second installs a secret remote Windows administration tool called "Back Orifice" that gives an unauthorized user access to your passwords, the ability to modify directories so that they can be shared on the network, and the ability to add and remove applications while remaining invisible to the user.

For more information, see the Internet Security Systems alert at **www.iss.net/xforce/alerts/advise5.html** and the Microsoft Security Bulletin at **www.microsoft.com/security/bulletins/ms98-010TEXT.htm**.

— *Warren Lampitt* is director of information systems at Gretmar Communications. Prior to founding that company, he was an information security officer with the Department of National Defence. Today he lectures extensively on network security and encryption.