NEXTSTEP

Title: Sendmail Patch Addendum
Entry Number: 1546
Last Updated: <<Date June 13 1995>>

The **sendmail** patch NeXT recently made available does not update the entire **sendmail** subsystem. In the original system software release, the files **/usr/bin/mailq** and **/usr/bin/newaliases** are *hard links: to the same file (i-node) as **/usr/lib/sendmail**. The patch replaces only the file called **/usr/lib/sendmail**, and does not affect the other two links. This leaves a system with the patch installed still open to some of the vulnerabilities addressed by the patch.

(**/usr/bin/mailq** provides a summary of the messages in the message queue,

and **/usr/bin/newaliases** regenerates the flat-file aliases database, which *is* referenced by **sendmail**.)

To close the vulnerabilities, follow the steps below.

1. Either log in as **root** and run the Terminal application, or, in a Terminal window, **su** to **root**.

2. Run the following commands (you type what's in **boldface**):

```
rhino-6# cd /usr/bin
rhino-7# rm mailq newaliases
rhino-8# ln -s ../lib/sendmail mailq
rhino-9# ln -s ../lib/sendmail newaliases
```

3. It is *not* necessary to reboot the computer, nor to restart the **sendmail** daemon.

The result of this procedure is to replace the old **mailq** and **newaliases** with relative symbolic links to the new **sendmail**.

This procedure should be performed on all NEXTSTEP computers on which the **sendmail** patch has been installed. Failure to complete the installation according to these instructions can result in your system remaining open to some of the vulnerabilities which the **sendmail** patch addresses.