

[Full-Disclosure] [RHSA-2003:039-06] Updated im packages fix insecure handling of temporary files

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-03/0054.html>

From: bugzilla@redhat.com

Date: 03/06/03

From: bugzilla@redhat.com

To: redhat-watch-list@redhat.com, redhat-announce-list@redhat.com

Date: Thu, 6 Mar 2003 10:09 -0500

Red Hat, Inc. Red Hat Security Advisory

Synopsis: Updated im packages fix insecure handling of temporary files

Advisory ID: RHSA-2003:039-06

Issue date: 2003-02-07

Updated on: 2003-03-06

Product: Red Hat Linux

Keywords: im tmp

Cross references:

Obsoletes:

CVE Names: CAN-2002-1395

1. Topic:

New im packages are available that fix the insecure handling of temporary files.

2. Relevant releases/architectures:

Red Hat Linux 7.0 – noarch

Red Hat Linux 7.1 – noarch

Red Hat Linux 7.2 – noarch

Red Hat Linux 7.3 – i386

Red Hat Linux 8.0 – i386

3. Problem description:

Internet Message (IM) is a series of user interface commands and backend Perl5 libraries that integrate email and the NetNews user interface. They are designed to be used from both the Mew mail reader for Emacs and the command line.

A vulnerability has been discovered by Tatsuya Kinoshita in the way two IM utilities create temporary files. By anticipating the names used to create files and directories stored in /tmp, it may be possible for a local attacker to corrupt or modify data as another user.

Red Hat Linux 7, 7.1, and 7.2 included IM packages that are vulnerable to this issue. This erratum includes IM version 143 which is not vulnerable to this issue.

Red Hat Linux 7.3, and 8.0 included Mew (Messaging in the Emacs World) packages which included vulnerable versions of IM. This erratum provide updated Mew packages including IM version 143 which is not vulnerable to this issue.

4. Solution:

Before applying this update, make sure all previously released errata relevant to your system have been applied.

To update all RPMs for your particular architecture, run:

```
rpm -Fvh [filenames]
```

where [filenames] is a list of the RPMs you wish to upgrade. Only those RPMs which are currently installed will be updated. Those RPMs which are not installed but included in the list will not be updated. Note that you can also use wildcards (*.rpm) if your current directory *only* contains the desired RPMs.

Please note that this update is also available via Red Hat Network. Many people find this an easier way to apply updates. To use Red Hat Network, launch the Red Hat Update Agent with the following command:

```
up2date
```

This will start an interactive process that will result in the appropriate RPMs being upgraded on your system.

5. RPMs required:

Red Hat Linux 7.0:

SRPMS:

<ftp://updates.redhat.com/7.0/en/os/SRPMS/im-143-0.7x.560.src.rpm>

noarch:

<ftp://updates.redhat.com/7.0/en/os/noarch/im-143-0.7x.560.noarch.rpm>

Red Hat Linux 7.1:

SRPMS:

<ftp://updates.redhat.com/7.1/en/os/SRPMS/im-143-0.7x.560.src.rpm>

noarch:

<ftp://updates.redhat.com/7.1/en/os/noarch/im-143-0.7x.560.noarch.rpm>

Red Hat Linux 7.2:

SRPMS:

<ftp://updates.redhat.com/7.2/en/os/SRPMS/im-143-1.src.rpm>

noarch:

<ftp://updates.redhat.com/7.2/en/os/noarch/im-143-1.noarch.rpm>

Red Hat Linux 7.3:

SRPMS:

<ftp://updates.redhat.com/7.3/en/os/SRPMS/mew-2.2-5.7x.src.rpm>

i386:

<ftp://updates.redhat.com/7.3/en/os/i386/mew-2.2-5.7x.i386.rpm>

<ftp://updates.redhat.com/7.3/en/os/i386/mew-common-2.2-5.7x.i386.rpm>

<ftp://updates.redhat.com/7.3/en/os/i386/mew-xemacs-2.2-5.7x.i386.rpm>

Red Hat Linux 8.0:

SRPMS:

<ftp://updates.redhat.com/8.0/en/os/SRPMS/mew-2.2-6.src.rpm>

i386:

<ftp://updates.redhat.com/8.0/en/os/i386/mew-2.2-6.i386.rpm>

<ftp://updates.redhat.com/8.0/en/os/i386/mew-common-2.2-6.i386.rpm>

<ftp://updates.redhat.com/8.0/en/os/i386/mew-xemacs-2.2-6.i386.rpm>

6. Verification:

MD5 sum Package Name

1339e1a6ccfafb1b92ca84ec211fb042 7.0/en/os/SRPMS/im-143-0.7x.560.src.rpm
02be12509784a2c1724648a10944b94a 7.0/en/os/noarch/im-143-0.7x.560.noarch.rpm
1339e1a6ccfafb1b92ca84ec211fb042 7.1/en/os/SRPMS/im-143-0.7x.560.src.rpm
02be12509784a2c1724648a10944b94a 7.1/en/os/noarch/im-143-0.7x.560.noarch.rpm
603fbef64e77847cab198ef21e95551e 7.2/en/os/SRPMS/im-143-1.src.rpm
86b3731ac5396768cbdfc55d71d75413 7.2/en/os/noarch/im-143-1.noarch.rpm
353574cd613a6acbd23d4b7acd32d8bd 7.3/en/os/SRPMS/mew-2.2-5.7x.src.rpm
826812ce71da4063b01e107557684638 7.3/en/os/i386/mew-2.2-5.7x.i386.rpm
3fe56a69a00556798de56e388f8a8d2c 7.3/en/os/i386/mew-common-2.2-5.7x.i386.rpm
bd7adf05659ef521c7b08ff9c702be54 7.3/en/os/i386/mew-xemacs-2.2-5.7x.i386.rpm
1f0574fe054426099cbae66b06435d8f 8.0/en/os/SRPMS/mew-2.2-6.src.rpm
3c6c2174a0bc0f0a1569af9d36f3c68d 8.0/en/os/i386/mew-2.2-6.i386.rpm
47b9bbd126fdd03298ebabe5a15f7806 8.0/en/os/i386/mew-common-2.2-6.i386.rpm

Full-Disclosure: [Full-Disclosure] [RHSA-2003:039-06] Updated im packages fix insecure handling of temporary files

41c228d865760c2a092fe1916c28d1d9 8.0/en/os/i386/mew-xemacs-2.2-6.i386.rpm

These packages are GPG signed by Red Hat, Inc. for security. Our key is available at <http://www.redhat.com/about/contact/pgpkey.html>

You can verify each package with the following command:

```
rpm --checksig -v <filename>
```

If you only wish to verify that each package has not been corrupted or tampered with, examine only the md5sum with the following command:

```
md5sum <filename>
```

7. References:

<http://www.debian.org/security/2002/dsa-202>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1395>

8. Contact:

The Red Hat security contact is [<security@redhat.com>](mailto:security@redhat.com). More contact details at <http://www.redhat.com/solutions/security/news/contact.html>

Copyright 2003 Red Hat, Inc.

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>