

# FreeBSD Security Advisory

## FreeBSD–SA–02:25.bzip2

**Source:** <http://www.derkeiler.com/Mailing–Lists/FreeBSD–Security/2002–05/9536.html>

---

**From:** FreeBSD Security Advisories ([security–advisories@freebsd.org](mailto:security–advisories@freebsd.org))

**Date:** 05/20/02

Date: Mon, 20 May 2002 09:08:14 –0700 (PDT)

From: FreeBSD Security Advisories <[security–advisories@freebsd.org](mailto:security–advisories@freebsd.org)>

To: FreeBSD Security Advisories <[security–advisories@freebsd.org](mailto:security–advisories@freebsd.org)>

-----BEGIN PGP SIGNED MESSAGE-----

=====  
FreeBSD–SA–02:25 Security Advisory

The FreeBSD Project

Topic: bzip2 contains multiple security vulnerabilities

Category: core/ports

Module: bzip2

Announced: 2002–05–20

Credits: Volker Schmidt, Philippe Troin

Affects: FreeBSD 4.4–RELEASE, FreeBSD 4.5–RELEASE,

FreeBSD 4.5–STABLE prior to the correction date.

bzip2 port prior to bzip2–1.0.2

Corrected: 2002–02–18 09:12:53 UTC (4.5–STABLE, RELENG\_4)

2002–02–23 18:28:09 UTC (4.5–RELEASE–p1, RELENG\_4\_5)

2002–02–23 18:33:18 UTC (4.4–RELEASE–p8, RELENG\_4\_4)

2002–02–22 13:21:22 UTC (bzip2 port)

FreeBSD only: NO

### I. Background

bzip2 is an advanced block–sorting file compression utility.

### II. Problem Description

When creating a file during decompression, the bzip2 utility failed to use the O\_EXCL flag, potentially overwriting files without warning.

In addition, the bzip2 utility did not securely create new files causing a race condition between creating the file and setting the correct permissions.

When compressing a file pointed to by a symbolic link, the bzip2 utility incorrectly stored the permissions of the symbolic link instead of the file. This may result in potentially lax file permissions (rwxr–xr–x), causing the decompressed file to be world–readable.

bzip2 was incorporated into FreeBSD prior to FreeBSD 4.4–RELEASE. Previous versions of FreeBSD did not contain bzip2 and are unaffected unless bzip2 was installed from the ports collection or manually by the system administrator.

### III. Impact

- 1) Files may be inadvertently overwritten without warning.
- 2) Due to the race condition between creating files and setting proper permissions, a local user may be able to read the contents of files regardless of their intended permissions.
- 3) Decompressed files that were originally pointed to by a symbolic link may end up with incorrect permissions, allowing local users to view their contents.

### IV. Workaround

- 1) Deinstall the bzip2 port/package if you have it installed.

### V. Solution

[FreeBSD 4.4 or 4.5 base system]

- 1) Upgrade your vulnerable system to 4.5–STABLE or the RELENG\_4\_4 or RELENG\_4\_5 security branch dated after the respective correction dates.

- 2) To patch your present system, download the relevant patch from the below location, and execute the following commands as root:

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:25/bzip2.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:25/bzip2.patch.asc
```

Verify the detached PGP signature using your PGP utility.

This patch has been verified to apply to FreeBSD 4.4–RELEASE and 4.5–RELEASE.

```
# cd /usr/src  
# patch -p < /path/to/patch  
# cd lib/libbz2  
# make depend && make all install  
# cd ../../usr.bin/bzip2  
# make depend && make all install
```

3) FreeBSD 4.4–RELEASE and 4.5–RELEASE systems:

An experimental upgrade package is available for users who wish to provide testing and feedback on the binary upgrade process. This package may be installed on FreeBSD 4.4–RELEASE and 4.5–RELEASE systems only, and is intended for use on systems for which source patching is not practical or convenient.

If you use the upgrade package, feedback (positive or negative) to [security-officer@FreeBSD.org](mailto:security-officer@FreeBSD.org) is requested so we can improve the process for future advisories.

During the installation procedure, backup copies are made of the files which are replaced by the package. These backup copies will be reinstalled if the package is removed, reverting the system to a pre-patched state.

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/packages/SA-02.25/security-patch-bzip2-02.25.tgz  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/packages/SA-02.25/security-patch-bzip2-02.25.tgz.asc
```

Verify the detached PGP signature using your PGP utility.

```
# pkg_add security-patch-bzip2-02.25.tgz
```

[ports]

1) Upgrade your entire ports collection and rebuild the bzip2 port.

2) Deinstall the old package and install a new package dated after the correction date, obtained from the following directories:

```
[i386]  
ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/archivers/  
ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-5-current/archivers/
```

[alpha]

Packages are not automatically generated for the alpha architecture at this time due to lack of build resources.

NOTE: It may be several days before updated packages are available. Be sure to check the file creation date on the package, because the version number of the software has not changed.

3) Download a new port skeleton for the bzip2 port from:

```
http://www.freebsd.org/ports/
```

and use it to rebuild the port.

4) Use the portcheckout utility to automate option (3) above. The portcheckout port is available in /usr/ports/devel/portcheckout or the

package can be obtained from:

<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages–4–stable/Latest/portcheckout.tgz>  
<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages–5–current/Latest/portcheckout.tgz>

## VI. Correction details

The following list contains the revision numbers of each file that was corrected in FreeBSD.

[Ports collection]

### Path Revision

---

ports/archivers/bzip2/Makefile 1.36  
ports/archivers/bzip2/distinfo 1.10  
ports/archivers/bzip2/pkg–descr 1.5  
ports/archivers/bzip2/pkg–plist 1.14

---

[Base system]

### Branch

#### Path Revision

### RELENG\_4

---

src/contrib/bzip2/CHANGES 1.1.1.1.2.2  
src/contrib/bzip2/FREEBSD–upgrade 1.1.2.1  
src/contrib/bzip2/LICENSE 1.1.1.1.2.2  
src/contrib/bzip2/Makefile 1.1.1.1.2.2  
src/contrib/bzip2/Makefile–libbz2\_so 1.1.1.1.2.2  
src/contrib/bzip2/README 1.1.1.1.2.2  
src/contrib/bzip2/README.COMPILATION.PROBLEMS 1.1.1.1.2.2  
src/contrib/bzip2/Y2K\_INFO 1.1.1.1.2.1  
src/contrib/bzip2/blocksort.c 1.1.1.1.2.2  
src/contrib/bzip2/bzip2.1 1.1.1.1.2.2  
src/contrib/bzip2/bzip2.c 1.1.1.1.2.2  
src/contrib/bzip2/bzip2recover.c 1.1.1.1.2.2  
src/contrib/bzip2/bzlib.c 1.1.1.1.2.2  
src/contrib/bzip2/bzlib.h 1.1.1.1.2.2  
src/contrib/bzip2/bzlib\_private.h 1.1.1.1.2.2  
src/contrib/bzip2/compress.c 1.1.1.1.2.2  
src/contrib/bzip2/crctable.c 1.1.1.1.2.2  
src/contrib/bzip2/decompress.c 1.1.1.1.2.2  
src/contrib/bzip2/dlltest.c 1.1.1.1.2.2  
src/contrib/bzip2/huffman.c 1.1.1.1.2.2  
src/contrib/bzip2/libbz2.def 1.1.1.1.2.1  
src/contrib/bzip2/makefile.msc 1.1.1.1.2.2  
src/contrib/bzip2/manual.texi 1.1.1.1.2.2  
src/contrib/bzip2/randtable.c 1.1.1.1.2.2  
src/contrib/bzip2/sample1.bz2.uu 1.1.1.1.2.2

```

src/contrib/bzip2/sample1.ref.gz.uu 1.1.1.1.2.2
src/contrib/bzip2/sample2.bz2.uu 1.1.1.1.2.2
src/contrib/bzip2/sample2.ref.gz.uu 1.1.1.1.2.1
src/contrib/bzip2/sample3.bz2.uu 1.1.1.1.2.2
src/contrib/bzip2/sample3.ref.gz.uu 1.1.1.1.2.1
src/contrib/bzip2/spewG.c 1.1.1.1.2.1
src/contrib/bzip2/unzcrash.c 1.1.1.1.2.1
src/contrib/bzip2/words0 1.1.1.1.2.1
src/contrib/bzip2/words1 1.1.1.1.2.1
src/contrib/bzip2/words2 1.1.1.1.2.1
src/contrib/bzip2/words3 1.1.1.1.2.2
RELENG_4_5
src/sys/conf/newvers.sh 1.44.2.20.2.2
src/contrib/bzip2/CHANGES 1.1.1.1.2.1.4.1
src/contrib/bzip2/FREEBSD–upgrade 1.1.4.1
src/contrib/bzip2/LICENSE 1.1.1.1.2.1.4.1
src/contrib/bzip2/Makefile 1.1.1.1.2.1.4.1
src/contrib/bzip2/Makefile–libbz2_so 1.1.1.1.2.1.4.1
src/contrib/bzip2/README 1.1.1.1.2.1.4.1
src/contrib/bzip2/README.COMPILATION.PROBLEMS 1.1.1.1.2.1.4.1
src/contrib/bzip2/Y2K_INFO 1.1.1.1.2.1
src/contrib/bzip2/blocksort.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/bzip2.1 1.1.1.1.2.1.4.1
src/contrib/bzip2/bzip2.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/bzip2recover.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/bzlib.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/bzlib.h 1.1.1.1.2.1.4.1
src/contrib/bzip2/bzlib_private.h 1.1.1.1.2.1.4.1
src/contrib/bzip2/compress.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/crc32table.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/decompress.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/dlltest.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/huffman.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/libbz2.def 1.1.1.1.2.1
src/contrib/bzip2/makefile.msc 1.1.1.1.2.1.4.1
src/contrib/bzip2/manual.texi 1.1.1.1.2.1.4.1
src/contrib/bzip2/randtable.c 1.1.1.1.2.1.4.1
src/contrib/bzip2/sample1.bz2.uu 1.1.1.1.2.1.4.1
src/contrib/bzip2/sample1.ref.gz.uu 1.1.1.1.2.1.4.1
src/contrib/bzip2/sample2.bz2.uu 1.1.1.1.2.1.4.1
src/contrib/bzip2/sample2.ref.gz.uu 1.1.1.1.2.1
src/contrib/bzip2/sample3.bz2.uu 1.1.1.1.2.1.4.1
src/contrib/bzip2/sample3.ref.gz.uu 1.1.1.1.2.1
src/contrib/bzip2/spewG.c 1.1.1.1.2.1
src/contrib/bzip2/unzcrash.c 1.1.1.1.2.1
src/contrib/bzip2/words0 1.1.1.1.2.1
src/contrib/bzip2/words1 1.1.1.1.2.1
src/contrib/bzip2/words2 1.1.1.1.2.1
src/contrib/bzip2/words3 1.1.1.1.2.1.4.1
RELENG_4_4
src/sys/conf/newvers.sh 1.44.2.17.2.7

```

src/contrib/bzip2/CHANGES 1.1.1.1.2.1.2.1  
src/contrib/bzip2/FREEBSD–upgrade 1.1.6.1  
src/contrib/bzip2/LICENSE 1.1.1.1.2.1.2.1  
src/contrib/bzip2/Makefile 1.1.1.1.2.1.2.1  
src/contrib/bzip2/Makefile–libbz2\_so 1.1.1.1.2.1.2.1  
src/contrib/bzip2/README 1.1.1.1.2.1.2.1  
src/contrib/bzip2/README.COMPILATION.PROBLEMS 1.1.1.1.2.1.2.1  
src/contrib/bzip2/Y2K\_INFO 1.1.1.1.2.1  
src/contrib/bzip2/blocksort.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/bzip2.1 1.1.1.1.2.1.2.1  
src/contrib/bzip2/bzip2.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/bzip2recover.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/bzlib.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/bzlib.h 1.1.1.1.2.1.2.1  
src/contrib/bzip2/bzlib\_private.h 1.1.1.1.2.1.2.1  
src/contrib/bzip2/compress.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/crc32table.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/decompress.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/dlltest.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/huffman.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/libbz2.def 1.1.1.1.2.1  
src/contrib/bzip2/makefile.msc 1.1.1.1.2.1.2.1  
src/contrib/bzip2/manual.texi 1.1.1.1.2.1.2.1  
src/contrib/bzip2/randtable.c 1.1.1.1.2.1.2.1  
src/contrib/bzip2/sample1.bz2.uu 1.1.1.1.2.1.2.1  
src/contrib/bzip2/sample1.ref.gz.uu 1.1.1.1.2.1.2.1  
src/contrib/bzip2/sample2.bz2.uu 1.1.1.1.2.1.2.1  
src/contrib/bzip2/sample2.ref.gz.uu 1.1.1.1.2.1  
src/contrib/bzip2/sample3.bz2.uu 1.1.1.1.2.1.2.1  
src/contrib/bzip2/sample3.ref.gz.uu 1.1.1.1.2.1  
src/contrib/bzip2/spewG.c 1.1.1.1.2.1  
src/contrib/bzip2/unzcrash.c 1.1.1.1.2.1  
src/contrib/bzip2/words0 1.1.1.1.2.1  
src/contrib/bzip2/words1 1.1.1.1.2.1  
src/contrib/bzip2/words2 1.1.1.1.2.1  
src/contrib/bzip2/words3 1.1.1.1.2.1.2.1

---

All files in src/contrib/bzip2 have identical revision numbers on their respective branches but do not contain the revision number in the source code.

## VII. References

<URL:<ftp://sources.redhat.com/pub/bzip2/docs/CHANGES>>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.7 (FreeBSD)

Comment: FreeBSD: The Power To Serve

FreeBSD–Security: FreeBSD Security Advisory FreeBSD–SA–02:25.bzip2

iQCVAwUBPOkduVUuHi5z0oilAQHJtAP/ZoPk981NwyoAzX+BIL9EM0JA19bYBSmp  
lgoSORQhK2Cu5DxqOt1J1Glu3748qrAU4+YkZ5JkucA6UgzDFd+mLcQbE57qrDCs  
rweqLHipm/fjQ8MXFbs5O2ZlrAPTauAiBYk60OtHEoYe5SE70By4zy8o0jzoKo8H  
5dXKGYTnve0=  
=UUGE  
-----END PGP SIGNATURE-----

To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org)  
with "unsubscribe freebsd–security" in the body of the message