

# FreeBSD Security Advisory

## FreeBSD–SA–05:14.bzip2

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-06/0032.html>

---

**From:** FreeBSD Security Advisories (*security-advisories\_at\_freebsd.org*)

**Date:** 06/29/05

Date: Wed, 29 Jun 2005 21:55:00 GMT

To: FreeBSD Security Advisories <security-advisories@freebsd.org>

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

Hash: SHA1

=====  
FreeBSD–SA–05:14.bzip2 Security Advisory  
The FreeBSD Project

Topic: bzip2 denial of service and permission race vulnerabilities

Category: contrib

Module: contrib\_bzip2

Announced: 2005–06–29

Credits: Imran Ghory, Chris Evans

Affects: All FreeBSD releases

Corrected: 2005–06–29 21:38:48 UTC (RELENG\_5, 5.4–STABLE)

2005–06–29 21:41:03 UTC (RELENG\_5\_4, 5.4–RELEASE–p3)

2005–06–29 21:42:33 UTC (RELENG\_5\_3, 5.3–RELEASE–p17)

2005–06–29 21:43:42 UTC (RELENG\_4, 4.11–STABLE)

2005–06–29 21:45:14 UTC (RELENG\_4\_11, 4.11–RELEASE–p11)

2005–06–29 21:46:15 UTC (RELENG\_4\_10, 4.10–RELEASE–p16)

CVE Name: CAN–2005–0953, CAN–2005–1260

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit

<URL:<http://www.freebsd.org/security/>>.

### I. Background

bzip2 is a block–sorting file compression utility.

### II. Problem Description

Two problems have been discovered relating to the extraction of bzip2–compressed files. First, a carefully constructed invalid bzip2

archive can cause bzip2 to enter an infinite loop. Second, when creating a new file, bzip2 closes the file before setting its permissions.

### III. Impact

The first problem can cause bzip2 to extract a bzip2 archive to an infinitely large file. If bzip2 is used in automated processing of untrusted files this could be exploited by an attacker to create an denial–of–service situation by exhausting disk space or by consuming all available cpu time.

The second problem can allow a local attacker to change the permissions of local files owned by the user executing bzip2 providing that they have write access to the directory in which the file is being extracted.

### IV. Workaround

Do not uncompress bzip2 archives from untrusted sources and do not uncompress files in directories where untrusted users have write access.

### V. Solution

Perform one of the following:

1) Upgrade your vulnerable system to 4–STABLE or 5–STABLE, or to the RELENG\_5\_4, RELENG\_5\_3, RELENG\_4\_11, or RELENG\_4\_10 security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 4.10, 4.11, 5.3, and 5.4 systems.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:14/bzip2.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:14/bzip2.patch.asc
```

b) Execute the following commands as root:

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

## VI. Correction details

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

## Branch Revision

## Path

-----  
RELENG\_4

contrib/bzip2/bzip2.c 1.1.1.1.2.3  
 contrib/bzip2/bzlib.c 1.1.1.1.2.3  
 contrib/bzip2/compress.c 1.1.1.1.2.3  
 contrib/bzip2/decompress.c 1.1.1.1.2.3  
 contrib/bzip2/huffman.c 1.1.1.1.2.3

## RELENG\_4\_11

src/UPDATING 1.73.2.91.2.12  
 src/sys/conf/newvers.sh 1.44.2.39.2.15  
 contrib/bzip2/bzip2.c 1.1.1.1.2.2.12.1  
 contrib/bzip2/bzlib.c 1.1.1.1.2.2.12.1  
 contrib/bzip2/compress.c 1.1.1.1.2.2.12.1  
 contrib/bzip2/decompress.c 1.1.1.1.2.2.12.1  
 contrib/bzip2/huffman.c 1.1.1.1.2.2.12.1

## RELENG\_4\_10

src/UPDATING 1.73.2.90.2.17  
 src/sys/conf/newvers.sh 1.44.2.34.2.18  
 contrib/bzip2/bzip2.c 1.1.1.1.2.2.10.1  
 contrib/bzip2/bzlib.c 1.1.1.1.2.2.10.1  
 contrib/bzip2/compress.c 1.1.1.1.2.2.10.1  
 contrib/bzip2/decompress.c 1.1.1.1.2.2.10.1  
 contrib/bzip2/huffman.c 1.1.1.1.2.2.10.1

## RELENG\_5

contrib/bzip2/bzip2.c 1.1.1.2.8.1  
 contrib/bzip2/bzlib.c 1.1.1.2.8.1  
 contrib/bzip2/compress.c 1.1.1.2.8.1  
 contrib/bzip2/decompress.c 1.1.1.2.8.1  
 contrib/bzip2/huffman.c 1.1.1.2.8.1

## RELENG\_5\_4

src/UPDATING 1.342.2.24.2.12  
 src/sys/conf/newvers.sh 1.62.2.18.2.8  
 contrib/bzip2/bzip2.c 1.1.1.2.12.1  
 contrib/bzip2/bzlib.c 1.1.1.2.12.1  
 contrib/bzip2/compress.c 1.1.1.2.12.1  
 contrib/bzip2/decompress.c 1.1.1.2.12.1  
 contrib/bzip2/huffman.c 1.1.1.2.12.1

## RELENG\_5\_3

src/UPDATING 1.342.2.13.2.20  
 src/sys/conf/newvers.sh 1.62.2.15.2.22  
 contrib/bzip2/bzip2.c 1.1.1.2.10.1  
 contrib/bzip2/bzlib.c 1.1.1.2.10.1  
 contrib/bzip2/compress.c 1.1.1.2.10.1  
 contrib/bzip2/decompress.c 1.1.1.2.10.1

contrib/bzip2/huffman.c 1.1.1.2.10.1

---

## VII. References

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0953>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1260>

<http://marc.theaimsgroup.com/?l=bugtraq&m=111229375217633>

<http://scary.beasts.org/security/CESA-2005-002.txt>

The latest revision of this advisory is available at

<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:14.bzip.asc>

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

Version: GnuPG v1.4.1 (FreeBSD)

iD8DBQFCwxenFdaIBMps37IRAsYxAJ9K8pFrImuACPxauHUqGqumKs2nLQCfQ0ne

SQ0RIXP6MiG88y/2B2wF7aA=

=TvEK

-----END PGP SIGNATURE-----

---

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"