

FreeBSD Security Advisory

FreeBSD-SA-05:18.zlib

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-07/0075.html>

From: FreeBSD Security Advisories (security-advisories_at_freebsd.org)

Date: 07/27/05

Date: Wed, 27 Jul 2005 08:50:54 GMT

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

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

Hash: SHA1

=====
FreeBSD-SA-05:18.zlib Security Advisory
The FreeBSD Project

Topic: Buffer overflow in zlib

Category: core

Module: libz

Announced: 2005-07-27

Credits: Markus Oberhumer

Affects: FreeBSD 5.3, FreeBSD 5.4

Corrected: 2005-07-27 08:41:44 UTC (RELENG_6, 6.0-BETA2)

2005-07-27 08:41:56 UTC (RELENG_5, 5.4-STABLE)

2005-07-27 08:42:16 UTC (RELENG_5_4, 5.4-RELEASE-p6)

2005-07-27 08:42:38 UTC (RELENG_5_3, 5.3-RELEASE-p20)

CVE Name: CAN-2005-1849

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/>>.

NOTE WELL: The issue discussed in this advisory is distinct from the issue discussed in the earlier advisory FreeBSD-SA-05:16.zlib, although the impact is very similar.

I. Background

zlib is a compression library used by numerous applications to provide data compression/decompression routines.

II. Problem Description

A fixed–size buffer is used in the decompression of data streams. Due to erroneous analysis performed when zlib was written, this buffer, which was believed to be sufficiently large to handle any possible input stream, is in fact too small.

III. Impact

A carefully constructed compressed data stream can result in zlib overwriting some data structures. This may cause applications to halt, resulting in a denial of service; or it may result in an attacker gaining elevated privileges.

IV. Workaround

No workaround is available.

V. Solution

Perform one of the following:

- 1) Upgrade your vulnerable system to 5–STABLE, or to the RELENG_5_4 or RELENG_5_3 security branch dated after the correction date.
- 2) To patch your present system:

The following patches have been verified to apply to FreeBSD 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-05:18/zlib.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:18/zlib.patch.asc
```

- b) Execute the following commands as root:

```
# cd /usr/src  
# patch < /path/to/patch  
# cd /usr/src/lib/libz/  
# 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_5	
src/lib/libz/inftrees.h	1.1.1.5.2.1

RELENG_5_4

src/UPDATING 1.342.2.24.2.15
src/sys/conf/newvers.sh 1.62.2.18.2.11
src/lib/libz/inftrees.h 1.1.1.5.6.1

RELENG_5_3

src/UPDATING 1.342.2.13.2.23
src/sys/conf/newvers.sh 1.62.2.15.2.25
src/lib/libz/inftrees.h 1.1.1.5.4.1

RELENG_6

src/lib/libz/inftrees.h 1.1.1.5.8.1

VII. References

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1849>

The latest revision of this advisory is available at

<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc>

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

Version: GnuPG v1.4.1 (FreeBSD)

iD4DBQFC50oLFdaIBMps37IRAg/1AJjTCluaNxJuBbSalLtgF34iey8DAJ9BGJmr
9NNdJfcjbm4qucvUYdsOqA==
=XDop

-----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"