

# [NEWS] Double Free Bug in zlib Compression Library

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0062.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/12/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Tue, 12 Mar 2002 22:21:11 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

Double Free Bug in zlib Compression Library

---

## SUMMARY

There is a bug in the zlib compression library that may manifest itself as a vulnerability in programs that are linked with zlib. This may allow an attacker to conduct a denial-of-service attack, gather information, or execute arbitrary code.

It is important to note that the CERT/CC has not received any reports of exploitation of this bug. Based on the information available to CERT at this time, it is difficult to determine whether this bug can be successfully exploited. However, given the widespread deployment of zlib, CERT has published this document as a proactive measure.

## DETAILS

Vulnerable systems:

\* Any software that is linked to zlib 1.1.3 or earlier may be affected

\* Data compression libraries derived from zlib 1.1.3 or earlier may contain a similar bug

## Securiteam: [NEWS] Double Free Bug in zlib Compression Library

There is a bug in the decompression algorithm used by the popular zlib compression library. If an attacker is able to pass a specially-crafted block of invalid compressed data to a program that includes zlib, the program's attempt to decompress the crafted data can cause the zlib routines to corrupt the internal data structures maintained by malloc.

The bug results from a programming error that causes segments of dynamically allocated memory to be released more than once (i.e., "double-freed"). Specifically, when `inftrees.c:huff_build()` encounters the crafted data, it returns an unexpected `Z_MEM_ERROR` to `inftrees.c:inflate_trees_dynamic()`. When a subsequent call is made to `inffblock.c:inflate_blocks()`, the `inflate_blocks` function tries to free an internal data structure a second time.

Because this bug interferes with the proper allocation and deallocation of dynamic memory, it may be possible for an attacker to influence the operation of programs that include zlib. In most circumstances, this influence will be limited to denial of service or information leakage, but it is theoretically possible for an attacker to insert arbitrary code into a running program. This code would be executed with the permissions of the vulnerable program.

The CERT/CC is tracking this issue as VU#368819. This reference number corresponds to CVE candidate CAN-2002-0059.

### Impact:

This bug may introduce vulnerabilities into any program that includes the affected library. Depending upon how and where the zlib routines are called from the given program, the resulting vulnerability may have one or more of the following impacts: denial of service, information leakage, or execution of arbitrary code.

### Solution:

Upgrade your version of zlib.

The maintainers of zlib have released version 1.1.4 to address this vulnerability. Upgrade any software that is linked to or derived from an earlier version of zlib. The latest version of zlib is available at <http://www.zlib.org> <http://www.zlib.org>.

The zlib compression library is freely available and used by many vendors in a wide variety of applications. Any one of these applications may contain vulnerabilities that are introduced by this vulnerability.

### Vendor Information:

## Securiteam: [NEWS] Double Free Bug in zlib Compression Library

This section contains information provided by vendors for this advisory.

If a particular vendor is not listed below, CERT/CC has not received their comments.

Apple Computer, Inc.

Mac OS X and Mac OS X Server do not contain this vulnerability.

Compaq Computer Corporation

x-ref: SSRT0818 zlib

At the time of writing this document, Compaq continues to evaluate this potential problem and impacts to Compaq released software. Compaq will implement solutions based on the conclusion of this evaluation as necessary. Compaq will provide notice of any new patches as a result any required solution through standard patch notification procedures and be available from your normal Compaq Services support channel.

Conectiva Linux

Conectiva Linux supported versions (5.0, 5.1, 6.0, 7.0, ferramentas graficas and ecommerce) are affected by the zlib vulnerability. Updates will be sent to our security mailing lists and be available at our ftp site and mirrors. The updates will include a new version of zlib itself and also other packages which include their own version of zlib or are linked statically to the system-wide copy of zlib.

Engarde

EnGarde Secure Linux Community and Professional are both vulnerable to the zlib bugs. Guardian Digital addressed this vulnerability in ESA-20020311-008 which may be found at:  
<[http://www.linuxsecurity.com/advisories/other\\_advisory-1960.html](http://www.linuxsecurity.com/advisories/other_advisory-1960.html)>  
[http://www.linuxsecurity.com/advisories/other\\_advisory-1960.html](http://www.linuxsecurity.com/advisories/other_advisory-1960.html)

EnGarde Secure Professional users may upgrade their systems using the Guardian Digital Secure Network.

FreeBSD

FreeBSD is not vulnerable, as the FreeBSD malloc implementation detects and complains about several programming errors including this kind of double free.

Fujitsu

Fujitsu's UXP/V operating system is not affected by the zlib vulnerability because it does not support zlib.

## Securiteam: [NEWS] Double Free Bug in zlib Compression Library

Hewlett-Packard Company

HP is not vulnerable.

IBM Corporation

IBM's AIX operating system, version 5.1, ships with open source-originated zlib that is used with the Redhat Package Manager (rpm) to install applications that are included in the AIX-Linux Affinity Toolkit. zlib (libz.a) is a shared library in AIX. AIX 5.1 is susceptible to the described vulnerability. AIX 4.3.x does not ship with zlib, but customers who install zlib and use it will be similarly vulnerable. IBM will make the patched version of zlib available as soon as it is made available to us.

OpenBSD

OpenBSD is not vulnerable as OpenBSD's malloc implementation detects double freeing of memory. The zlib shipped with OpenBSD has been fixed in OpenBSD-current in January 2002.

Openwall GNU/\*/Linux

All versions of Openwall GNU/\*/Linux (Owl) prior to the 2002/02/15 Owl-current snapshot are affected by the zlib double-free vulnerability. Owl-current after 2002/02/15 includes the proper fixes in its userland packages. In order to not place the users of other vendors' products at additional risk, we have agreed to delay documenting this as a security change and including the fixes in Owl 0.1-stable until there's a coordinated public announcement. While we don't normally support this kind of a policy (releasing a fix before there's an announcement), this time handling the vulnerability in this way was consistent with the state of things by the time the (already publicly known) bug was first realized to be a security vulnerability.

The zlib bug could affect the following Owl packages: gnupg, openssh, rpm, texinfo (not necessarily in a security sense). Of these, the OpenSSH could potentially allow for an active remote attack resulting in a root compromise. If only SSH protocol version 1 is allowed in the OpenSSH server this is reduced to a local attack, but reverse remote attack possibilities by a malicious server remain. Additionally, any third-party software that makes use of the provided zlib library could be affected.

Parts of the Linux 2.2 kernel included in Owl were also affected by the vulnerability. Fortunately, those parts (Deflate compression support for PPP and the experimental Deflate compression extension to IrDA) are normally not used by the Owl userland. The bug has been corrected starting with Linux 2.2.20-ow2 which has been made public and a part of both Owl-current and Owl 0.1-stable on 2002/03/03. This change, however, will only be documented in the publicly-available change logs on the

## Securiteam: [NEWS] Double Free Bug in zlib Compression Library

coordinated public announcement date.

Red Hat, Inc.

Red Hat Linux ships with a zlib library that is vulnerable to this issue. Although most packages in Red Hat Linux use the shared zlib library we have identified a number of packages that either statically link to zlib or contain an internal version of the zlib code.

Updates to zlib and these packages as well as our advisory note are available from the following URL. Users of the Red Hat Network can use the up2date tool to automatically upgrade their systems.

<<http://www.redhat.com/support/errata/RHSA-2002-026.html>>  
<http://www.redhat.com/support/errata/RHSA-2002-026.html>

Red Hat would like to thank CERT/CC for their help in coordinating this issue with other vendors.

SGI

SGI acknowledges the zlib vulnerabilities reported by CERT and is currently investigating. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported IRIX operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on

<<http://www.sgi.com/support/security/>>  
<http://www.sgi.com/support/security/>.

XFree86

XFree86 versions 4.0 through 4.2.0 include zlib version 1.0.8. XFree86 3.x includes zlib version 1.0.4. The zlib code included with XFree86 is only used on some platforms. This is determined by the setting of HasZlib in the imake config files in the xc/config/cf source directory. If HasZlib is set to YES in the platform's vendor.cf file(s), then the system-provided zlib is used instead of the XFree86-provided version. XFree86 uses the system-provided zlib by default only on the following platforms:

FreeBSD 2.2 and later  
NetBSD 1.2.2 and later

## Securiteam: [NEWS] Double Free Bug in zlib Compression Library

OpenBSD  
Darwin  
Debian Linux

The zlib code in XFree86 has been fixed in the CVS repository (trunk and the xf-4\_2-branch branch) as of 14 February 2002. A source patch for XFree86 4.2.0 will be available from

<<ftp://ftp.xfree86.org/pub/XFree86/4.2.0/fixes/>>  
<ftp://ftp.xfree86.org/pub/XFree86/4.2.0/fixes/>.

The following XFree86 4.2.0 binary distributions provided by XFree86 include and use a vulnerable version of zlib:

Linux-alpha-glibc22  
Linux-ix86-glibc22

When updated binaries are available, it'll be documented at

<<http://www.xfree86.org/4.2.0/UPDATES.html>>  
<http://www.xfree86.org/4.2.0/UPDATES.html>.

To check if an installation of XFree86 includes zlib, see if the following file exists:

/usr/X11R6/lib/libz.a

To check if an XFree86 X server is dynamically linked with zlib, look for a line containing 'libz' in the output of 'ldd /usr/X11R6/bin/XFree86'.

Various vendors repackage and distribute XFree86, and may use settings and configurations different from those described here.

[zlib.org](http://zlib.org)

All users of zlib versions 1.1.3 or earlier should obtain the latest version, 1.1.4 or later, from <http://www.zlib.org>, in order to avoid this vulnerability as well as other possible vulnerabilities in versions prior to 1.1.3 when decompressing invalid data.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:cert@cert.org>> CERT/CC.

### References:

- \* <[http://bugzilla.gnome.org/show\\_bug.cgi?id=70594](http://bugzilla.gnome.org/show_bug.cgi?id=70594)>  
[http://bugzilla.gnome.org/show\\_bug.cgi?id=70594](http://bugzilla.gnome.org/show_bug.cgi?id=70594)
- \* <<http://www.kb.cert.org/vuls/id/368819>>  
<http://www.kb.cert.org/vuls/id/368819>
- \* <<http://www.libpng.org/pub/png/pngapps.html>>  
<http://www.libpng.org/pub/png/pngapps.html>
- \* <<http://www.redhat.com/support/errata/RHSA-2002-026.html>>

Securiteam: [NEWS] Double Free Bug in zlib Compression Library

<http://www.redhat.com/support/errata/RHSA-2002-026.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Windows Shell Overflow (Additional Information)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)