CERT Advisory CA-2002-07 Double Free Bug in zlib Compression Library

Original release date: March 12, 2002
Last revised: July 20, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- 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

Overview

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 us at this time, it is difficult to determine whether this bug can be successfully exploited. However, given the widespread deployment of zlib, we have published this document as a proactive measure.

I. Description

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:huft_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 infblock.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.

II. 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.

III. 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

These are the MD5 checksums for zlib version 1.1.4:

> *abc405d0bdd3ee22782d7aa20e440f08 zlib-1.1.4.tar.gz*
> *9bf1d36ced334b0cf1f996f5c8171018 zlib114.zip*

The maintainers of zlib have published an advisory regarding this issue; for further information, please see

> *http://www.gzip.org/zlib/advisory-2002-03-11.txt*

Apply a patch from your vendor

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.

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

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

Cisco Systems

Cisco Systems is addressing the vulnerability identified by VU#368819 across all affected products. Cisco has released an advisory:

> *http://www.cisco.com/warp/public/707/zlib-double-free.shtml*

Compaq Computer Corporation

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.

COMPAQ COMPUTER CORPORATION

Conectiva Linux

Conectiva Linux supported versions (5.0, 5.1, 6.0, 7.0, ferramentas graficas and ecomerce) 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.

Debian

Users of Debian GNU/Linux 2.2 (potato) should upgrade to zlib version 1.1.3-5.1. More information is available at http://www.debian.org/security/2002/dsa-122. Note that a few packages which include private copies of zlib will also need to be upgraded--more information is available at the above link.

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*

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.

F-Secure Corporation

F-Secure SSH is not vulnerable to zlib double free bug.

No version of F-Secure SSH software is vulnerable to the "Double Free Bug in zlib Compression Library" discussed in CERT Advisory CA-2002-07.

All F-Secure SSH versions, both the old SSH1 and later SSH2 protocol clients and servers, close connection immediately with fatal cleanup call without any further calls to zlib when call to zlib's inflate() returns something else than Z_OK.

Fujitsu

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

Hewlett-Packard Company

Some HP-UX software (for example, X and lbxproxy) is linked with the 1.0.8 version of zlib. This version came before the introduction of the reported double free problem and is not vulnerable.

Other HP-UX software (for example, OpenSSH) is linked with the latest zlib (1.1.4) and is not vulnerable.

IBM Corporation

IBM's AIX operating system, version 5.1, ships with open source-originated zlib that is used with the Red Hat 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 presumed susceptible to the described vulnerability, though we have not demonstrated exploitability yet. AIX 4.3.x does not ship with zlib, but customers who install zlib and use it may be similarly vulnerable.

The updated zlib package can be downloaded by directing your browser to:

> *http://oss.software.ibm.com/developerworks/projects/aixtoolbox*

The updated rpm package can be downloaded from:

> *ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte*

Juniper Networks

Juniper Networks has completed an initial assessment of this vulnerability, and we believe that our implementation is not susceptible. Test programs show that our memory allocation algorithm correctly detects and warns about any attempt to exploit the vulnerability described in the CERT/CC advisory.

We continue to evaluate the risks associated with this vulnerability. If we determine that the JUNOS software is susceptible, we will quickly issue any patches or software updates required to maintain the security of Juniper Networks routers.

Future JUNOS software releases will include a corrected version of the libz code.

Microsoft Corporation

Microsoft conducted a thorough source-code level review of its products in response to the reports of vulnerabilities in zlib. This review did not discover any vulnerabilities related to these reports.

NetBSD

NetBSD's malloc libraries are not vulnerable to double-free() attacks. The updated zlib will be included in future releases, but a Security Advisory will not be issued.

Novell, Inc.

Novell is working on a fix for Novell JVM for NetWare 1.3.1. We will post the fix in the May NDK. Version 1.4 will also have the fix in it. We will also update this statement with the URL to download the fix.

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.

OpenSSH

OpenSSH itself relies on zlib as a third party library. OpenSSH's internal malloc state might get corrupted if the double-free bug is present in zlib. At this moment, it is not known if this bug will allow an intruder to gain privileges.

For some malloc implementation it is possible to detect and ignore the double-free. However, that is entirely dependent on the malloc implementation. Currently, it seems that *BSD operating systems might not be affected by this problem.

We advise everybody to upgrade their third party libraries and recompile OpenSSH if necessary. Turning off compression in the server is possible only by removing zlib from myproposal.h and subsequent recompliation.

```
Index: myproposal.h
===================================================================
RCS file: /cvs/src/usr.bin/ssh/myproposal.h,v
retrieving revision 1.13
diff -u -r1.13 myproposal.h
--- myproposal.h        21 Jan 2002 22:30:12 -0000      1.13
+++ myproposal.h        12 Mar 2002 17:36:11 -0000
@@ -32,7 +32,7 @@
        "hmac-md5,hmac-sha1,hmac-ripemd160," \
        "hmac-ripemd160@openssh.com," \
        "hmac-sha1-96,hmac-md5-96"
-#define        KEX_DEFAULT_COMP        "none,zlib"
 !)+#define        KEX_DEFAULT_COMP        "none"
 #define        KEX_DEFAULT_LANG        ""
```

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 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*

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/.

SSH Communications Security

SSH Secure Shell is not vulnerable to zlib double free bug.

No version of SSH Secure Shell software is vulnerable to the "Double Free Bug in zlib Compression Library" discussed in CERT Advisory CA-2002-07.

All SSH Secure Shell versions, including SSH2 protocol clients and servers, close the connection immediately with a fatal cleanup call without any further calls to zlib when a call to zlib's inflate() returns something else than Z_OK.

Standard Networks, Inc.

Standard Networks offers a "mainframe connectivity" product called "OpenIT" which uses the zlib library to compress ("zip") files transferred between Unisys mainframes and remote FTP clients and servers. After a code analysis we found the zlib vulnerability does not affect this product.

Standard Networks also offers a secure HTTPS-based file transfer client called "MOVEit Wizard" which uses the zlib library to compress ("zip") files transferred between MOVEit DMZ servers and remote browsers. After a code analysis we found the zlib vulnerability does not affect this product.

Nonetheless, Standard Networks will use "corrected" versions of zlib in future versions of both products.

No other Standard Networks products ("ActiveHEAT","EMU","MOVEit DMZ", "MOVEit Central", "MOVEit Admin", "MOVEit Freely", "MOVEit Buddy", "Unigate") are affected.

Customers are encouraged to call Standard Networks immediately (+001 608.227.6100) with any questions or concerns about their specific configuration.

Sun Microsystems, Inc.

Solaris 8 includes the zlib library as part of the SUNWzlib package which is affected by this issue. Open Windows 3.6.1 (for Solaris 7) and Open Windows 3.6.2 (for Solaris 8) ship a version of zlib which is affected in recent patches. Sun has produced patches for both Solaris and Open Windows which address this issue. The impact and patch details are described in Sun Alert 43541 available here:

> *http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F43541*

SuSE Linux AG

All SuSE Linux versions previous to 8.0 are affected by this issue. We have released security updates for zlib itself, as well as several packages including their own copy of zlib.

Details on this issue, as well as the list of packages to upgrade, can be found in our advisory at:

> *http://www.suse.de/de/support/security/2002_010_libz_txt.html*
> *http://www.suse.de/de/support/security/2002_011_libz_packages_txt.html*

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*
> *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/.

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.

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

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.

Appendix B. - References

- http://bugzilla.gnome.org/show_bug.cgi?id=70594
- http://www.gzip.org/zlib/advisory-2002-03-11.txt
- http://www.kb.cert.org/vuls/id/368819

- http://www.libpng.org/pub/png/pngapps.html
- http://www.redhat.com/support/errata/RHSA-2002-026.html
- http://www.securityfocus.com/bid/4267

The CERT/CC thanks Owen Taylor and Mark Cox of Red Hat, Inc. for reporting this vulnerability. We also thank Mark Adler of zlib.org for contributing to our research and Matthias Clasen for contributing to the discovery of this vulnerability.

This document was written by Jeffrey P. Lanza.

Revision History

```
Mar 12, 2002:  Initial release
Mar 14, 2002:  Added references to zlib advisory
Mar 15, 2002:  Added Microsoft statement
Mar 15, 2002:  Added NetBSD statement
Mar 15, 2002:  Added F-Secure statement
Mar 18, 2002:  Added Debian statement
Mar 18, 2002:  Added Standard Networks statement
Mar 21, 2002:  Added SSH Communications statement
Mar 21, 2002:  Added Sun Microsystems statement
Mar 29, 2002:  Added Juniper Networks statement; updated Hewlett-Packard statement
Apr 03, 2002:  Added Cisco statement
Apr 14, 2002:  Added Novell statement; updated Hewlett-Packard statement
May 02, 2002:  Updated Microsoft statement
May 06, 2002:  Added SuSE Linux AG statement
Jun 17, 2002:  Updated Sun Microsystems statement
Jun 24, 2002:  Added OpenSSH statement
Jun 25, 2002:  Updated IBM statement
Jul 20, 2002:  Updated Hewlett-Packard statement
```