CERT Advisory CA-1997-11 Vulnerability in libXt

Original issue date: May 1, 1997
Last revised: January 5, 1998
Added vendor information for SGI.

A complete revision history is at the end of this file.

There have been discussions on public mailing lists about buffer overflows in the Xt library of the X Windowing System made freely available by The Open Group (and previously by the now-defunct X Consortium). The specific problem outlined in those discussions was a buffer overflow condition in the Xt library, and the file xc/lib/Xt/Error.c. Exploitation scripts were made available.

Since then (the latter half of 1996), The Open Group has extensively reviewed the source code for the entire distribution to address the potential for further buffer overflow conditions. These conditions can make it possible for a local user to execute arbitrary instructions as a privileged user without authorization.

The programs that pose a potential threat to sites are those programs that have been built from source code prior to X11 Release 6.3 and have setuid or setgid bits set. Some third-party vendors distribute derivatives of the X Window System, and if you use a distribution that includes X tools that have setuid or setgid bits set, you may be vulnerable as well.

The CERT/CC team recommends upgrading to X11 Release 6.3 or installing a patch from your vendor. If you cannot do one of these, then as a last resort we recommend that you remove the setuid or setgid bits from any executable files contained in your distribution of X; this may have an adverse effect on some system operations.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

There have been discussions on public mailing lists about buffer overflows in the Xt library of the X Windowing System made freely available by The Open Group (and previously by the now-defunct X Consortium). During these discussions, exploitation scripts were made available for some platforms.**

The specific problem outlined in those discussions was a buffer overflow condition in the Xt library and the file xc/lib/Xt/Error.c. It was possible for a user to execute arbitrary instructions as a privileged user using a program built by this distribution with setuid or setgid bits set.

Note that in this case a root compromise was only possible when programs built from this distribution (e.g., xterm) were setuid root.
Since then The Open Group has extensively reviewed the source code for the entire distribution to address the potential for further buffer overflow condition.

If you use a distribution of the X Windowing System earlier than X11 Release 6.3 that you downloaded and compiled yourself, we encourage you to take the steps outlined in either Section IV A or C.

If you use third-party vendor-supplied distributions of the X Windowing System containing setuid root programs, we encourage you to take the steps outlined in Sections IV B or C.

** Note: Discussions of this specific instance of the vulnerability appeared on mailing lists during the second half of 1996. Exploitation scripts were made public at that time.

II. Impact

Platforms that have X applications built with the setuid or setgid bits set may be vulnerable to buffer overflow conditions. These conditions can make it possible for a local user to execute arbitrary instructions as a privileged user without authorization. Access to an account on the system is necessary for exploitation.

III. Finding Potentially Vulnerable Distributions

A. For Sites That Download and Build Their Own Distributions

As discussed earlier, the programs that pose a potential threat to sites are those programs that have been built from source code, prior to X11 Release 6.3 and have setuid or setgid bits set.

Sites that have downloaded the X source code from the X Consortium should be able to identify such programs by looking in the directory hierarchy defined by the "ProjectRoot" constant described in the xc/config/cf/site.def file in the source code distribution. The default is /usr/X11R6.3. The X11R6.3 Installation Guide states:

"ProjectRoot

> The destination where X will be installed. This variable needs to be set before you build, as some programs that read files at run-time have the installation directory compiled in to them. Assuming you have set the variable to some value /path, files will be installed into /path/bin, /path/include /X11, /path/lib, and /path/man."

B. For Vendor-Supplied Distributions

Some third-party vendors distribute derivatives of the X Window System. If you use a distribution that includes X tools that have setuid or setgid bits set, then you may need to apply Solution B or C in Section IV.

If you use a distribution that does not have setuid or setgid bits enabled on any X tools, then you do not need to take any of the steps listed below.

Below is a list of vendors who have provided information about this problem. If your vendor's name is not on this list and you need clarification, you should check directly with your vendor.

IV. Solution

If any X tools that you are using are potentially vulnerable (see Section III), we encourage you to take one of the following steps. If the setuid or setgid bits are not enabled on any of the tools in your distribution, you do not need to take any of the steps listed below.

For distributions that were built directly from the source code supplied by The Open Group (and previously by the X Consortium), we encourage you to apply either Solutions A or C. For vendor-supplied distributions, we encourage you to apply either Solutions B or C.

A. Upgrade to X11 Release 6.3

If you download and build your own distributions directly from the source code, we encourage you to install the latest version, X11 Release 6.3. The source code can be obtained from

ftp://ftp.x.org/pub/R6.3/tars/xc-1.tar.gz
ftp://ftp.x.org/pub/R6.3/tars/xc-2.tar.gz
ftp://ftp.x.org/pub/R6.3/tars/xc-3.tar.gz

Note that these distributions are very large. The compressed files consume about 40M of disk space. The uncompressed tar files consume about 150M of disk space.

B. Install a patch from your vendor

Below is a list of vendors who have provided information about this problem. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Data General Corporation
Digital Equipment Corporation (DEC)
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
NEC Corporation
NeXT Software, Inc.
The Open Group (formerly OSF/X Consortium)
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics, Inc.
Sun Microsystems, Inc.

C. Remove the setuid bit from affected programs

If you are unable to apply Solutions A or B, then as a last resort we recommend removing the setuid or setgid bits from the executable files in your distribution of X.

Note that this may have an adverse effect on some system operations. For instance, on some systems the xlock program needs to have the setuid bit enabled so that the shadow password file can be read to unlock the screen. By removing the setuid bit from this program, you remove the ability of the xlock program to read the shadow password file. This means that particular version of the xlock program should not be used at all, or it should be killed from another terminal when necessary.

Appendix A - Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

We released a patch for this for the 2.1 BSD/OS release,
and it's already fixed in our current release.

Data General Corporation

All versions of DG/UX are vulnerable.

Patches for this vulnerability are in progress.

Digital Equipment Corporation (DEC)

At the time of writing this document, patches(binary kits) are in progress and final testing is expected to begin soon. Digital will provide notice of the completion/availability of the patches through AES services (DIA, DSNlink FLASH) and be available from your normal Digital Support channel.

FreeBSD, Inc.

We're aware of the problem and are trying to correct it with a new release of the Xt library.

Hewlett-Packard Company

HPSBUX9704-058
Description: Security Vulnerability in libXt for HP-UX 9.X & 10.X
HEWLETT-PACKARD SECURITY BULLETIN: #00058 libXt

Security Bulletins are available from the HP Electronic
Support Center via electronic mail.

Use your browser to get to the HP Electronic Support
Center page at:

http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America)

http://europe-support.external.hp.com (for Europe)

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:
APAR - IX61784,IX67047,IX66713 (PTF - U445908,U447740)

To determine if you have this PTF on your system, run the following command:
lslpp -lB U445908 U447740

AIX 4.1

Apply the following fix to your system:
APAR - IX61031 IX66736 IX66449

To determine if you have this APAR on your system, run the following command:

instfix -ik IX61031 IX66736 IX66449

Or run the following command:

lslpp -h X11.base.lib

Your version of X11.base.lib should be 4.1.5.2 or later.

AIX 4.2

Apply the following fix to your system:

APAR - IX66824 IX66352

To determine if you have this APAR on your system, run the following command:

instfix -ik IX66824 IX66352

Or run the following command:

lslpp -h X11.base.lib

Your version of X11.base.lib should be 4.2.1.0 or later.

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://service.software.ibm.com/aixsupport/

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

NEC Corporation

EWS-UX/V(Rel4.2) R7.x - R10.x	vulnerable
EWS-UX/V(Rel4.2MP) R10.x	vulnerable
UP-UX/V(Rel4.2MP) R5.x - R7.x	vulnerable
UX/4800 R11.x - current	vulnerable

Patches for this vulnerability are in progress.
For further information, please contact by e-mail:

UX48-security-support@nec.co.jp

NeXT Software, Inc.

X-Windows is not part of any NextStep or OpenStep release. We are not vulnerable to this problem.

The Open Group (formerly OSF/X Consortium)
Not vulnerable.

The Santa Cruz Operation, Inc. (SCO)
We are investigating this problem and will provide updated
information for this advisory when it becomes available.

Silicon Graphics, Inc.
Silicon Graphics Inc. has investigated the issue and recommends the following steps for neutralizing the exposure. It is HIGHLY RECOMMENDED that these measures be implemented on ALL SGI systems. This issue will be corrected in future releases of IRIX.

For further information, please refer to Silicon Graphics Inc. Security Advisory Number: 19971101-01-PX, "libXt Security Issues."

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp /security and ~ftp/patches directories, respectfully.

Sun Microsystems, Inc.
Bulletin Number: #00153
Date: August 25, 1997
Title: Vulnerabilities in libXt
Vulnerable: SunOS versions 5.5.1, 5.5.1_x86, 5.5, 5.5_x86, 5.4, 5.4_x86, 5.3, 4.1.4, and 4.1.3_U1
The vulnerabilities are fixed in Solaris 2.6.

Patches are available to all Sun customers via World Wide Web at:

ftp://sunsolve1.sun.com/pub/patches/patches.html;

Customers with Sun support contracts can also obtain patches from local Sun answer centers and SunSITEs worldwide.

Sun security bulletins are available via World Wide Web at:

http://sunsolve1.sun.com/sunsolve/secbulletins

Revision History

```
Jan. 5, 1998  Added vendor information for Silicon Graphics, Inc.
Dec. 11, 1997 Appendix A - updated vendor information for Data General Corporation.
Sep. 26, 1997 Updated copyright statement
Aug. 27, 1997 Appendix A - updated vendor information for Sun Microsystems,Inc.
May 8, 1997   Appendix A - updated vendor information for Hewlett-Packard.
```