IOActive Security Advisory

Protocol Handling Issues in X.Org X Window System Client Libraries
May 24, 2013

Affected Products

X Window System Client Libraries

Affected Versions

X.Org believes all prior versions of these libraries contain the vulnerabilities discussed in this document, dating back to their introduction.

Versions of the X libraries built on top of the Xlib bridge to the XCB framework are vulnerable to fewer issues than those without. This is due to the added safety and consistency assertions in the XCB calls to read data from the network. However, most of these vulnerabilities are not caught by such checks.

Technical Details

Ilja van Sprundel, a security researcher with IOActive, discovered a large number of issues relating to the way that various X client libraries handle the responses they receive from servers. Mr. van Sprundel worked with X.Org's security team to analyze, confirm, and fix these issues.

Most of the issues stem from the client libraries trusting the server to send the correct protocol data without verifying that the values will not overflow or cause other damage. Often, the X clients and servers are run by the same user, with the server being more privileged than the clients, but this is not an issue.

Scenarios exist in which a privileged client can be connected to an unprivileged server. For example, connecting a setuid X client (such as a screen lock program) to a virtual X server (such as Xyfb or Xephyr) that has been modified by the user to return data may allow the user to escalate privileges.

The X.Org security team would like to take this opportunity to remind X client authors that current best practices suggest separating code that requires privileges from the GUI to reduce the attack surface issues such as the one mentioned above.

Integer Overflows Calculation Vulnerability

A vulnerability exists involving integer overflows when calculating memory needs for replies. These calls do not verify that their calculations for determining how much money is needed to handle the returned data have not overflowed. This can result in allocating an insufficient amount of memory and then writing the returned data beyond the end of the allocated buffer.

Affected Library	Affected Functions
CVE-2013-XXXX: libX11 1.5.99.901 (1.6 RC1) and earlier	Affected functions: • XQueryFont() • _XF86BigfontQueryFont() • XListFontsWithInfo() • XGetMotionEvents() • XListHosts() • XGetModifierMapping() • XGetPointerMapping() • XGetKeyboardMapping()
CVE-2013-XXXX: libXext 1.3.1 and earlier	Affected functions: • XcupGetReservedColormapEntries() • XcupStoreColors() • XdbeGetVisualInfo() • XeviGetVisualInfo() • XShapeGetRectangles() • XSyncListSystemCounters()
CVE-2013-XXXX: libXfixes 5.0 and earlier	Affected functions: • XFixesGetCursorImage()
CVE-2013-XXXX: libXi 1.7.1 and earlier	Affected functions: • XGetDeviceControl() • XGetFeedbackControl() • XGetDeviceDontPropagateList() • XGetDeviceMotionEvents() • XIGetProperty() • XIGetSelectedEvents() • XGetDeviceProperty()
CVE-2013-XXXX: libXinerama 1.1.2 and earlier	Affected functions: • XineramaQueryScreens()

CVE-2013-XXXX: libXrandr 1.4.0 and earlier	Affected functions: • XRRQueryOutputProperty() • XRRQueryProviderProperty(). This function was introduced in libXrandr 1.4.0 and is not found in 1.3.2 and older releases.
CVE-2013-XXXX: libXrender 0.9.7 and earlier	Affected functions: • XRenderQueryFilters() • XRenderQueryFormats() • XRenderQueryPictIndexValues()
CVE-2013-XXXX: libXRes 1.0.6 and earlier	Affected functions: • XResQueryClients() • XResQueryClientResources()
CVE-2013-XXXX: libXv 1.0.7 and earlier	Affected functions: • XvQueryPortAttributes() • XvListImageFormats() • XvCreateImage()
CVE-2013-XXXX: libXvMC 1.0.7 and earlier	Affected functions: • XvMCListSurfaceTypes() • XvMCListSubpictureTypes()
CVE-2013-XXXX: libXxf86dga 1.1.3 and earlier	Affected functions: • XDGAQueryModes() • XDGASetMode()
CVE-2013-XXXX: libdmx 1.1.2 and earlier	Affected functions: • DMXGetScreenAttributes() • DMXGetWindowAttributes() • DMXGetInputAttributes()

CVE-2013-XXXX: libGLX in Mesa 9.1.1 and earlier	Affected functions: • XF86DRIOpenConnection() • XF86DRIGetClientDriverName()
CVE-2013-XXXX: libchromeXvMC and libchromeXvMCPro in openChrome 0.3.2 and earlier	Affected functions: • uniDRIOpenConnection() • uniDRIGetClientDriverName()

Sign Extension Memory Calculation Vulnerability

A vulnerability exists which involves sign extension issues in calculating the memory needs for replies. These calls do not verify that their calculations for how much memory is needed to handle the returned data have not had sign extension issues when converting smaller integers to larger ones. This leads to the use of negative numbers in memory size calculations that can result in allocating too little memory and then writing the returned data past the end of the allocated buffer.

Affected Library	Affected Functions
CVE-2013-XXXX: libXi 1.7.1 and earlier	Affected functions: • XListInputDevices()
CVE-2013-XXXX: libFS 1.0.4 and earlier	Affected functions: • FSOpenServer()

Buffer Overflow Vulnerability

A vulnerability exists involving buffer overflows resulting from not validating the length or offset values in replies. Calls do not verify that the length and/or indexes returned by the server are within the bounds specified by the caller or the bounds of the memory allocated by the function. As a result, when storing returned data, it is possible to write beyond the bounds of the allocated memory.

Affected Library	Affected Functions
CVE-2013-XXXX: libX11 1.5.99.901 (1.6 RC1) and earlier	Affected functions: • XAllocColorCells() • _XkbReadGetDeviceInfoReply() • _XkbReadGeomShapes() • _XkbReadGetGeometryReply() • _XkbReadKeySyms() • _XkbReadKeyActions() • _XkbReadKeyBehaviors() • _XkbReadModifierMap() • _XkbReadExplicitComponents() • _XkbReadVirtualModMap() • _XkbReadGetNamesReply() • _XkbReadGetMapReply() • _XimXGetReadData() • XListFonts() • XListExtensions()
CVE-2013-XXXX: libXi 1.7.1 and earlier	Affected functions: • XGetDeviceButtonMapping() • _XIPassiveGrabDevice()
CVE-2013-XXXX: libXvMC 1.0.7 and earlier	Affected functions: • XvMCGetDRInfo()
CVE-2013-XXXX: libXxf86dga 1.1.3 and earlier	Affected functions: • XF86VidModeGetGammaRamp()
CVE-2013-XXXX: libXxf86vm 1.1.2 and earlier	Affected functions: • XDGAQueryModes() • XDGASetMode()
CVE-2013-XXXX: libXt 1.1.3 and earlier	Affected function: • _XtResourceConfigurationEH()

Integer Overflow Parsing Vulnerability

A vulnerability exists that involves integer overflows when parsing user-specified files. Calls do not verify that their calculations for how much memory is needed to handle the data being read have not overflowed. This can result in the allocation of insufficient memory and writing the returned data beyond the end of the allocated buffer.

Affected Library	Affected Functions
CVE-2013-XXXX: libX11 1.5.99.901 (1.6 RC1) and earlier	Affected functions: • LoadColornameDB() • XrmGetFileDatabase() • _XimParseStringFile() • TransFileName()
CVE-2013-XXXX: libXcursor 1.1.13 and earlier	Affected functions: • _XcursorFileHeaderCreate()

Unbounded Recursion Parsing Vulnerability

A vulnerability exists that involves the unbounded recursion parsing of user-specified files. Calls read in files and handle C-style "#include" directives to include other files. They have no limit for how many levels deep they will go. (This includes allowing files to #include themselves.) Eventually, the stack overflows from the recursive function calling patterns.

Affected Library	Affected Functions
CVE-2013-XXXX: libX11 1.5.99.901 (1.6 RC1) and earlier	Affected functions: • GetDatabase() • _XimParseStringFile()

Memory Corruption Vulnerability

A vulnerability exists that involves memory corruption due to unchecked return values. Calls assume that pointers are properly initialized by the XGetWindowProperty() function and do not check for failure of the function to return a valid window property. This can lead to the use of uninitialized pointers for reading, writing, or passing to functions such as free().

XGetWindowProperty() in libX11 1.5.99.901 (1.6RC1) and earlier did not ensure that returned pointers were initialized to NULL when returning a failure. (This is fixed in libX11 1.5.99.902 and later.)

Affected Library	Affected Functions
CVE-2013-XXXX: libXt 1.1.3 and earlier	Affected functions: • ReqCleanup() • HandleSelectionEvents() • ReqTimedOut() • HandleNormal() • HandleSelectionReplies()

Integer Overflows Calculating Memory Needs for Replies Vulnerability

A vulnerability exists that involves integer overflows when calculating memory needs for replies. These calls do not confirm whether their calculations (for how much memory is needed to handle the returned data) are resulting in overflows. An insufficient amount of memory may be allocated, and returned data may be written beyond the end of the allocated buffer.

Affected Library	Affected Functions
CVE-2013-1981: libX11 1.5.99.901 (1.6 RC1) and earlier	Affected functions: • XQueryFont() • _XF86BigfontQueryFont() • XListFontsWithInfo() • XGetMotionEvents() • XListHosts() • XGetModifierMapping() • XGetPointerMapping() • XGetKeyboardMapping() • XGetWindowProperty() • XGetImage()
CVE-2013-1982: libXext 1.3.1 and ealier	Affected functions: • XcupGetReservedColormapEntries() • XcupStoreColors() • XdbeGetVisualInfo() • XeviGetVisualInfo() • XShapeGetRectangles() • XSyncListSystemCounters()
CVE-2013-1983: libXfixes 5.0 and earlier	Affected functions: • XFixesGetCursorImage()
CVE-2013-1984: libXi 1.7.1 and earlier	Affected functions: • XGetDeviceControl() • XGetFeedbackControl() • XGetDeviceDontPropagateList() • XGetDeviceMotionEvents() • XIGetProperty() • XIGetSelectedEvents() • XGetDeviceProperties() • XListInputDevices()
CVE-2013-1985:	Affected functions:

libXinerama 1.1.2 and earlier	• XineramaQueryScreens()
CVE-2013-2062: libXp 1.0.1 and earlier	Affected functions: • XpGetAttributes() • XpGetOneAttribute() • XpGetPrinterList() • XpQueryScreens()
CVE-2013-1986: libXrandr 1.4.0 and earlier	Affected functions: • XRRQueryOutputProperty() • XRRQueryProviderProperty() [XRRQueryProviderProperty() was introduced in libXrandr 1.4.0 and is not found in 1.3.2 and older releases.]
CVE-2013-1986 libXrandr 1.4.0 and earlier	Affected functions:
CVE-2013-1987: libXrender 0.9.7 and earlier	Affected functions: • XRenderQueryFilters() • XRenderQueryFormats() • XRenderQueryPictIndexValues()
CVE-2013-1988: libXRes 1.0.6 and earlier	Affected functions: • XResQueryClients() • XResQueryClientResources()
CVE-2013-2063: libXtst 1.2.1 and earlier	Affected functions: XRecordGetContext()
CVE-2013-1989: libXy 1.0.7 and earlier	Affected functions: • XyQueryPortAttributes() • XyListImageFormats() • XyCreateImage()
CVE-2013-1990: libXyMC	Affected functions:

1.0.7 and earlier	• XyMCListSurfaceTypes() • XyMCListSubpictureTypes()
CVE-2013-1991: libXxf86dga 1.1.3 and earlier	Affected functions: • XDGAQueryModes() • XDGASetMode()
CVE-2013-1992: libdmx 1.1.2 and earlier	Affected functions: • DMXGetScreenAttributes() • DMXGetWindowAttributes() • DMXGetInputAttributes()
CVE-2013-2064: libxcb 1.9 and earlier	Affected functions: read_packet()
CVE-2013-1993: libGLX in Mesa 9.1.1 and earlier	Affected functions: • XF86DRIOpenConnection() • XF86DRIGetClientDriverName()
CVE-2013-1994: libchromeXyMC and libchromeXyMCPro in openChrome 0.3.2 and earlier	Affected functions: • uniDRIOpenConnection() • uniDRIGetClientDriverName()

Sign Extension Issues Calculating Memory Needs for Replies Vulnerability

A vulnerability exists that involves sign extension issues calculating memory needs for replies. These calls do not confirm that their calculations (for how much memory is needed to handle the returned data) have not had sign extension issues when converting smaller integer types to larger ones. This leads to negative numbers being used in memory size calculations. As a result, an insufficient amount of memory may be allocated, and returned data may be written beyond the end of the allocated buffer.

Affected Library	Affected Functions
CVE-2013-1995: libXi 1.7.1 and earlier	Affected functions: • XListInputDevices()
CVE-2013-1996: libFS 1.0.4 and earlier	Affected functions: • FSOpenServer()

Buffer Overflows Due to Not Validating Length or Offset Values in Replies Vulnerability

A vulnerability exists that involves buffer overflows caused by not validating the length or offset values in replies. These calls do not confirm that the lengths and/or indices returned by the server are within the bounds specified by the caller or the bounds of the allocated memory of that function. As a result, the returned data can be written beyond the bounds of the allocated memory during storage.

Affected Library	Affected Functions
CVE-2013-1997: libX11 1.5.99.901 (1.6 RCI) and earlier	Affected functions: • XAllocColorCells() • _XkbReadGetDeviceInfoReply() • _XkbReadGeomShapes() • _XkbReadGetGeometryReply() • _XkbReadKeySyms() • _XkbReadKeyActions() • _XkbReadKeyBehaviors() • _XkbReadModifierMap() • _XkbReadExplicitComponents() • _XkbReadVirtualModMap() • _XkbReadGetNamesReply() • _XkbReadGetMapReply() • _XimXGetReadData() • XListFonts() • XListExtensions() • XGetFontPath()
CVE-2013-1998: libXi 1.7.1 and earlier	Affected functions: • XGetDeviceButtonMapping() • _XIPassiveGrabDevice() • XQueryDeviceState()
CVE-2013-2006: libXy 1.0.7 and earlier	Affected functions: • XyQueryPortAttributes()
CVE-2013-1999: libXyMC 1.0.7 and earlier	Affected functions: • XyMCGetDRInfo()
CVE-2013-2000: libXxf8dga 1.1.3 and earlier	Affected functions: • XDGAQueryModes() • XDGASetMode()
CVE-2013-2001: libXxf86vm	Affected functions:

1.1.2 and earlier	• XF86VidModeGetGammaRamp()
CVE-2013-2002: libXt 1.1.3 and earlier	Affected functions: • _XtResourceConfigurationEH()

Integer Overflows Parsing User-specified File Replies Vulnerability

A vulnerability exists that involves integer overflows parsing of user-specified file replies. These calls do not confirm that their calculations (for how much memory is needed to handle the data being read) have not overflowed. As a result, an insufficient amount of memory may be allocated, and returned data may be written beyond the end of the allocated buffer.

Affected Library	Affected Functions
CVE-2013-1981: libX11 1.5.99.901 (1.6 RC1) and earlier	Affected functions: • LoadColornameDB() • XrmGetFileDatabase() • _XimParseStringFile() • TransFileName()
CVE-2013-2003: libXcursor 1.1.13 and earlier	Affected functions: • _XcursorFileHeaderCreate()

Unbounded Recursion Parsing User-specified Files Vulnerability

A vulnerability exists that involves the unbounded recursion parsing of user-specified files. These calls read in files and handle C-style #include directives to include other files. They have no limit for how many levels deep they can go and allow files to #include themselves, until the stack overflows from the recursive function calling patterns.

Affected Library	Affected Functions
CVE-2013-2004: libX11 1.5.99.901 (1.6 RC1) and earlier	Affected functions: • GetDatabase() • _XimParseStringFile()

Memory Corruption Due to Unchecked Return Values Vulnerability

A vulnerability exists involving memory corruption to the unchecked return values. These calls assume that pointers are properly initialized by the XGetWindowProperty() function and do not check for failure of the function to return a valid window property. This can lead to the use of uninitialized pointers for reading, writing, or passing functions, such as free().

XGetWindowProperty() in libX11 1.5.99.901 (1.6 RC1) and earlier does not ensure that returned pointers were initialized to NULL when returning a failure. (This is fixed in libX11 1.5.99.902 and later.)

Affected Library	Affected Functions
CVE-2013-2005: libXt 1.1.3 and earlier	Affected functions: • ReqCleanup() • HandleSelectionEvents() • ReqTimedOut() • HandleNormal() • HandleSelectionReplies()

Affected Versions

X.Org believes all prior versions of these libraries contain these flaws, dating back to their introduction.

Versions of the X libraries built on top of the Xlib bridge to the XCB framework are vulnerable to fewer issues than those without. This is due to the added safety and consistency assertions in the XCB calls to read data from the network. However, most of these vulnerabilities are not caught by those checks.

Fixes

Fixes are available in git commits and patches. These will be listed at:

http://www.x.org/wiki/Development/Security/Advisory-2013-05-23

when this advisory is released.

Fixes will also be included in these module releases from X.Org:

- libX11 1.5.99.902 (1.6 RC2)
- libXcursor 1.1.14
- libXext 1.3.2
- libXfixes 5.0.1
- libXi 1.7.2
- libXinerama 1.1.3
- libXp 1.0.2
- libXrandr 1.4.1
- libXrender 0.9.8
- libXRes 1.0.7

- libXv 1.0.8
- libXvMC 1.0.8
- libXxf86dga 1.1.4
- libXxf86vm 1.1.3
- libdmx 1.1.3
- libxcb 1.9.1
- libFS 1.0.5
- libXt 1.1.4

or in releases to be determined based on our sister projects:

- xf86-video-openchrome. OpenChrome project - http://www.openchrome.org/
- Mesa. Mesa3D project - http://www.mesa3d.org/

Thanks

X.Org thanks Ilja van Sprundel of IOActive for reporting these issues to our security team and assisting us with understanding the issues and evaluating our fixes. We would also like to thank Alan Coopersmith of Oracle for coordinating the X.Org response and developing the fixes for these issues.