IOActive Security Advisory

Title	**Protocol Handling Issues in X Window System Servers**
Severity	Medium/High
Discovered by	Ilja van Sprundel
Advisory Date	December 9, 2014

Affected Products

1. X server
2. Other products that use GLX indirect rendering code from Silicon Graphics, Inc.

Impact

An attacker could exploit the vulnerabilities to cause the X server to access uninitialized memory or overwrite arbitrary memory in the X server process. This can cause a denial of service (e.g., an X server segmentation fault), which can prevent the use of the machine. An attacker also could potentially execute arbitrary code.

An X server is a program in the X Window System that handles access to graphics cards, display screens, and input devices on local machines.

Background

Ilja van Sprundel, a security researcher with IOActive, has discovered a large number of issues in the way the X server codebase handles requests from X clients, and has worked with X.Org's security team to analyze, confirm, and fix these issues.

Ilja's talk at the 30th Chaos Communication Congress (30C3) in Hamburg, Germany, last year ("X Security: It's worse than it looks") provided a preview of these issues and discussed the general form of many, but did not disclose exact details.

The criticality of these vulnerabilities increases if the X server runs with root privileges, is exposed to network clients, and/or has permission to use affected protocol extensions, especially the GLX extension.

Technical Details

X.Org believes all versions of the affected functions contain these flaws, dating back to their introduction. The following Common Vulnerabilities and Exposures (CVEs) identify the release of X Window System (known as X11) or other software in which the CVE was introduced.

We've listed the earliest date of any affected function in a given protocol or area, but some functions may have been introduced later.

Denial of Service Due to Unchecked Malloc in Client Authentication

CVE-2014-8091: Servers Built with Support for SUN-DES-1 (Secure RPC)

In servers built with support for SUN-DES-1 authorization credentials (based on Secure RPC), an unauthenticated client may be able to crash the X server by sending a connection request that specifies values that cause malloc to fail. The malloc failure then causes the authentication routines to attempt to write data to the returned NULL pointer.

Since the request is limited to an unsigned 16-bit integer for the allocation size, it is unlikely to fail unless the server is severely memory constrained.

Introduced in the initial revision of Secure RPC support in X11R5 (1991).

Integer Overflows Due to Calculating Memory Needs for Requests

These calls perform length calculations to determine how much memory is needed to handle the client's request. However, the calls do not check for integer overflows when performing these calculations, which can result in out-of-bounds reads or writes. The calls all occur only after a client has successfully authenticated itself.

CVE-2014-8092: X11 Core Protocol Requests

Affected functions: ProcPutImage(), GetHosts(), RegionSizeof(), REQUEST_FIXED_SIZE()

Introduced in X11R1 (1987)

CVE-2014-8093: GLX Extension

Affected functions: __glXDisp_ReadPixels(), __glXDispSwap_ReadPixels(), __glXDisp_GetTexImage(), _glXDispSwap_GetTexImage(), GetSeparableFilter(), GetConvolutionFilter(), GetHistogram(), GetMinmax(), GetColorTable(), __glXGetAnswerBuffer(), __GLX_GET_ANSWER_BUFFER(), __glXMap1dReqSize(), __glXMap1fReqSize(), Map2Size(), __glXMap2dReqSize(), __glXMap2fReqSize(), __glXImageSize(), __glXSeparableFilter2DReqSize()

The GLX extension to the X Window System allows an X client to send X protocol to the X server, to request that the X server perform OpenGL rendering on behalf of the X client. This is known as "GLX indirect rendering." It differs from "GLX direct rendering" where the X client submits OpenGL rendering commands directly to the GPU; direct rendering bypasses the X server and avoids the X server code for GLX protocol handling.

Most GLX indirect rendering implementations share some common ancestry, dating back to "Sample Implementation" code from Silicon Graphics, Inc. (SGI), which SGI originally commercially licensed to other Unix workstation and graphics vendors. SGI released it as open source in 1999.

GLX indirect rendering is included in X.Org releases beginning with X11R6.7 (2004) and XFree86 releases beginning with XFree86 4.0 (2000). XFree86 is an implementation of the X Window System.

Note: IOActive did not test software released by other licensees of SGI's code base, which might also be vulnerable.

CVE-2014-8094: DRI2 Extension

Affected functions: ProcDRI2GetBuffers()

Introduced in xorg-server-1.7.0 (2009)

Out-of-bounds Access Due to Not Validating Length or Offset Values in Requests

These calls do not check to make sure that the lengths and/or indexes sent by the client are within the bounds specified by the caller or the bounds of the memory allocated to hold the request read from the client, so could read or write past the bounds of allocated memory while processing the request. All of these calls occur only after a client has successfully authenticated itself.

CVE-2014-8095: XInput extension

Affected functions: SProcXChangeDeviceControl(), ProcXChangeDeviceControl(), ProcXChangeFeedbackControl(), ProcXSendExtensionEvent(), SProcXIAllowEvents(), SProcXIChangeCursor(), ProcXIChangeHierarchy(), SProcXIGetClientPointer(), SProcXIGrabDevice(), SProcXIUngrabDevice(), ProcXIUngrabDevice(), SProcXIPassiveGrabDevice(), ProcXIPassiveGrabDevice(), SProcXIPassiveUngrabDevice(), ProcXIPassiveUngrabDevice(), SProcXListDeviceProperties(), SProcXDeleteDeviceProperty(), SProcXIListProperties(), SProcXIDeleteProperty(), SProcXIGetProperty(), SProcXIQueryDevice(), SProcXIQueryPointer(), SProcXISelectEvents(), SProcXISetClientPointer(), SProcXISetFocus(), SProcXIGetFocus(), SProcXIWarpPointer()

Introduced in X11R4 (1989)

CVE-2014-8096: XC-MISC Extension

Affected functions: SProcXCMiscGetXIDList()

Introduced in X11R6.0 (1994)

CVE-2014-8097: DBE Extension

Affected functions: ProcDbeSwapBuffers(), SProcDbeSwapBuffers()

Introduced in X11R6.1 (1996)

CVE-2014-8098: GLX Extension

Affected functions: __glXDisp_Render(), __glXDisp_RenderLarge(), __glXDispSwap_VendorPrivate(), __glXDispSwap_VendorPrivateWithReply(), set_client_info(), __glXDispSwap_SetClientInfoARB(), DoSwapInterval(), DoGetProgramString(), DoGetString(), __glXDispSwap_RenderMode(), __glXDisp_GetCompressedTexImage(), __glXDispSwap_GetCompressedTexImage(), __glXDisp_FeedbackBuffer(), __glXDispSwap_FeedbackBuffer(), __glXDisp_SelectBuffer(), __glXDispSwap_SelectBuffer(), __glXDisp_Flush(), __glXDispSwap_Flush(), __glXDisp_Finish(), __glXDispSwap_Finish(), __glXDisp_ReadPixels(), __glXDispSwap_ReadPixels(), __glXDisp_GetTexImage(), __glXDispSwap_GetTexImage(), __glXDisp_GetPolygonStipple(), __glXDispSwap_GetPolygonStipple(), __glXDisp_GetSeparableFilter(), __glXDisp_GetSeparableFilterEXT(), __glXDisp_GetConvolutionFilter(), __glXDisp_GetConvolutionFilterEXT(), __glXDisp_GetHistogram(), __glXDisp_GetHistogramEXT(), __glXDisp_GetMinmax(), __glXDisp_GetMinmaxEXT(), __glXDisp_GetColorTable(), __glXDisp_GetColorTableSGI(), GetSeparableFilter(), GetConvolutionFilter(), GetHistogram(), GetMinmax(), GetColorTable()

Originally developed by SGI, it was licensed to multiple vendors before SGI open sourced the code in 1999

Introduced in XFree86 4.0.0 (2000)

Introduced in X11R6.7 (2004)

CVE-2014-8099: XVideo Extension

Affected functions: SProcXvQueryExtension(), SProcXvQueryAdaptors(), SProcXvQueryEncodings(), SProcXvGrabPort(), SProcXvUngrabPort(), SProcXvPutVideo(), SProcXvPutStill(), SProcXvGetVideo(), SProcXvGetStill(), SProcXvPutImage(), SProcXvShmPutImage(), SProcXvSelectVideoNotify(), SProcXvSelectPortNotify(), SProcXvStopVideo(), SProcXvSetPortAttribute(), SProcXvGetPortAttribute(), SProcXvQueryBestSize(), SProcXvQueryPortAttributes(), SProcXvQueryImageAttributes(), SProcXvListImageFormats()

Introduced in XFree86 4.0.0 (2000)

Introduced in X11R6.7 (2004)

CVE-2014-8100: Render Extension

Affected functions: ProcRenderQueryVersion(), SProcRenderQueryVersion(), SProcRenderQueryPictFormats(), SProcRenderQueryPictIndexValues(), SProcRenderCreatePicture(), SProcRenderChangePicture(), SProcRenderSetPictureClipRectangles(), SProcRenderFreePicture(), SProcRenderComposite(), SProcRenderScale(), SProcRenderCreateGlyphSet(), SProcRenderReferenceGlyphSet(), SProcRenderFreeGlyphSet(), SProcRenderFreeGlyphs(), SProcRenderCompositeGlyphs()

Introduced in XFree86 4.0.1 (2000)

Introduced in X11R6.7 (2004)

CVE-2014-8101: RandR Extension

Affected functions: SProcRRQueryVersion(), SProcRRGetScreenInfo(), SProcRRSelectInput(), SProcRRConfigureOutputProperty()

Introduced in XFree86 4.2.0 (2002)

Introduced in X11R6.7 (2004)

CVE-2014-8102: XFixes Extension

Affected functions: SProcXFixesSelectSelectionInput()

Introduced in X11R6.8.0 (2004)

CVE-2014-8103: DRI3 and Present Extensions

Affected functions: sproc_dri3_query_version(), sproc_dri3_open(), sproc_dri3_pixmap_from_buffer(), sproc_dri3_buffer_from_pixmap(), sproc_dri3_fence_from_fd(), sproc_dri3_fd_from_fence(), proc_present_query_capabilities(), sproc_present_query_version(), sproc_present_pixmap(), sproc_present_notify_msc(), sproc_present_select_input(), sproc_present_query_capabilities()

Introduced in xorg-server-1.15.0 (2013)

Fixes

For the X.Org project, fixes are available in git commits and patches will be available when released at http://www.x.org/wiki/Development/Security. In addition, X.Org is planning to incorporate fixes into the xorg-server-1.17.0 and xorg-server-1.16.3 releases.

Mitigation

While the fixes cover all the cases currently known to X.Org, this does not protect against exposure to similar issues. For additional protection, use these methods:

- Configure the X server to prohibit X connections from the local area network (by passing the "-nolisten tcp" command line option to the X.Org X server). Many OS distributions are already set this way by default. Consult the OS's documentation for details on setting X server command line options.
- Disable GLX indirect contexts. Some implementations have a configuration option for this. In xorg-server-1.16 and later releases, this can be achieved by setting the '-iglx' X server command line option. This option is the default in xorg-server-1.17 and later releases.

Timeline

- Late December 2013 – IOActive discovers vulnerability
- November 25, 2014 – IOActive sent draft advisory and patch files to the distros@openwall list
- December 9, 2014 – IOActive advisory published

Acknowledgments

IOActive acknowledges the following X.Org contributors, who developed and reviewed the X Server fixes and coordinated the X.Org response to them:

- Adam Jackson (Red Hat)
- Alan Coopersmith (Oracle)
- Andy Ritger (NVIDIA)
- Julien Cristau (Debian)
- Keith Packard (Intel)
- Michal Srb (SuSE)
- Peter Hutterer (Red Hat)
- Robert Morell (NVIDIA)