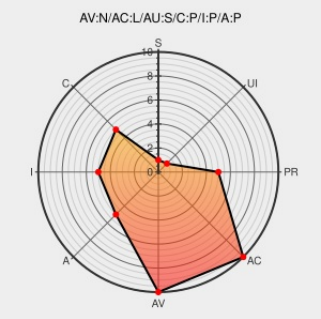
CVE-2014-8103

Published on: 12/10/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:42:00 AM UTC

CVE-2014-8103

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xorg-server from X.org contain the following vulnerability:

X.Org Server (aka xserver and xorg-server) 1.15.0 through 1.16.x before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) sproc_dri3_query_version, (2) sproc_dri3_open, (3) sproc_dri3_pixmap_from_buffer, (4) sproc_dri3_buffer_from_pixmap, (5) sproc_dri3_fence_from_fd, (6) sproc_dri3_fd_from_fence, (7) proc_present_query_capabilities, (8) sproc_present_query_version, (9) sproc_present_pixmap, (10) sproc_present_notify_msc, (11) sproc_present_select_input, or (12) sproc_present_query_capabilities function in the (a) DRI3 or (b) Present extension.

CVE-2014-8103 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Oracle Bulletin Board Update - January 2015	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
CVE-2014-8103 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2014-8103
Advisory 2014-12-09	Patch	CONFIRM

Advisory-2014-12-09	Patch Vendor Advisory www.x.org text/html	CONFIRM www.x.org/wiki/Development/Security/Advisory-2014-12-09/
Security Advisory SA61947 - SUSE update for xorg-x11-server - Secunia	web.archive.org text/html	SECUNIA 61947
1168716 – (CVE-2014-8103) CVE-2014-8103 xorg-x11-server: out of bounds access due to not validating length or offset values in DRI3 & Present extensions	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1168716
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:1983
X.Org X Server: Multiple vulnerabilities (GLSA 201504-06) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201504-06

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	X.org	Xorg-server	1.15.0	All	All	All
Application	X.org	Xorg-server	1.15.0.901	All	All	All
Application	X.org	Xorg-server	1.15.1	All	All	All
Application	X.org	Xorg-server	1.15.2	All	All	All
Application	X.org	Xorg-server	1.15.99.901	All	All	All
Application	X.org	Xorg-server	1.15.99.902	All	All	All
Application	X.org	Xorg-server	1.15.99.903	All	All	All
Application	X.org	Xorg-server	1.15.99.904	All	All	All
Application	X.org	Xorg-server	1.16.0	All	All	All
Application	X.org	Xorg-server	1.16.0.901	All	All	All
Application	X.org	Xorg-server	1.16.1	All	All	All
Application	X.org	Xorg-server	1.16.1.901	All	All	All
Application	X.org	Xorg-server	1.16.2	All	All	All
Application	X.org	Xorg-server	1.16.2.901	All	All	All
Application	X.org	Xorg-server	1.16.2.99.901	All	All	All
Application	X.org	Xorg-server	1.15.0	All	All	All
Application	X.org	Xorg-server	1.15.0.901	All	All	All
Application	X.org	Xorg-server	1.15.1	All	All	All

Application	X.org	Xorg-server	1.15.2	All	All	All
Application	X.org	Xorg-server	1.15.99.901	All	All	All
Application	X.org	Xorg-server	1.15.99.902	All	All	All
Application	X.org	Xorg-server	1.15.99.903	All	All	All
Application	X.org	Xorg-server	1.15.99.904	All	All	All
Application	X.org	Xorg-server	1.16.0	All	All	All
Application	X.org	Xorg-server	1.16.0.901	All	All	All
Application	X.org	Xorg-server	1.16.1	All	All	All
Application	X.org	Xorg-server	1.16.1.901	All	All	All
Application	X.org	Xorg-server	1.16.2	All	All	All
Application	X.org	Xorg-server	1.16.2.901	All	All	All
Application	X.org	Xorg-server	1.16.2.99.901	All	All	All

cpe:2.3:a:x.org:xorg-server:1.15.0:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.0.901:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.1:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.2:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.99.901:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.99.902:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.99.903:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.99.904:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.16.0:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.16.0.901:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.16.1:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.16.1.901:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.16.2:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.16.2.901:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.16.2.99.901:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.0:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.0.901:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.1:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.2:*:*:*:*:*:*:*:

cpe:2.3:a:x.org:xorg-server:1.15.99.901:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.15.99.902:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.15.99.903:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.15.99.904:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.16.0:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.16.0.901:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.16.1:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.16.1.901:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.16.2:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.16.2.901:*:*:*:*:*:*:*

cpe:2.3:a:x.org:xorg-server:1.16.2.99.901:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→