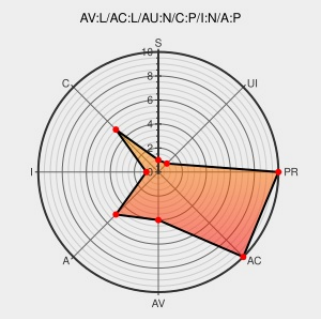
CVE-2010-4819

Published on: 09/05/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:12:01 AM UTC

CVE-2010-4819

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



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

The ProcRenderAddGlyphs function in the Render extension (render/render.c) in X.Org xserver 1.7.7 and earlier allows local users to read arbitrary memory and possibly cause a denial of service (server crash) via unspecified vectors related to an "input sanitization flaw."

CVE-2010-4819 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 3.6 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
Bug 28801 – Missing input sanitation in ProcRenderAddGlyphs triggers SEGV	bugs.freedesktop.org text/html	CONFIRM bugs.freedesktop.org/show_bug.cgi?id=28801
oss-security - Re: CVE Request: X.org ProcRenderGlyps input sanitation issue	www.openwall.com text/html	MLIST [oss-security] 20110923 Re: CVE Request: X.org ProcRenderGlyps input sanitation issue
	aix.software.ibm.com text/plain	CONFIRM aix.software.ibm.com/aix/efixes/security/X_advisory2.asc
oss-security - CVE Request: X.org ProcRenderGlyps input sanitation issue	www.openwall.com text/html	MLIST [oss-security] 20110922 CVE Request: X.org ProcRenderGlyps input sanitation issue
xorg/xserver - X server (mirrored from https://gitlab.freedesktop.org/xorg/xserver)	cgit.freedesktop.org text/html	CONFIRM cgit.freedesktop.org/xorg/xserver/commit/render/render.c?id=5725849a1b427cd4a72b84e57f211edb35838718
X Input Validation Flaw in ProcRenderAddGlyphs()	securitytracker.com	SECTRACK 1026149

Lets Local Users Obtain Memory Contents and Deny Service - SecurityTracker	text/html	
access.redhat.com	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2011:1360
access.redhat.com	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2011:1359

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	X	X.org-xserver	1.7	All	All	All
Application	X	X.org-xserver	1.7.6.902	All	All	All
Application	X	X.org-xserver	1.7.7	rc2	All	All
Application	X	X.org-xserver	1.7	All	All	All
Application	X	X.org-xserver	1.7.6.902	All	All	All
Application	X	X.org-xserver	1.7.7	rc2	All	All
Application	X	X.org-xserver	All	All	All	All

cpe:2.3:a:x:x.org-xserver:1.7:*:*:*:*:*:*:*:

cpe:2.3:a:x:x.org-xserver:1.7.6.902:*:*:*:*:*:*:*:

cpe:2.3:a:x:x.org-xserver:1.7.7:rc2:*:*:*:*:*:*:*:

cpe:2.3:a:x:x.org-xserver:1.7:*:*:*:*:*:*:*:

cpe:2.3:a:x:x.org-xserver:1.7.6.902:*:*:*:*:*:*:*:

cpe:2.3:a:x:x.org-xserver:1.7.7:rc2:*:*:*:*:*:*:*:

cpe:2.3:a:x:x.org-xserver:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report