



# CVE-2006-1526

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2006-1526
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-05-02 21:06:00 UTC
<b>Updated</b>	2018-10-18 16:33:00 UTC
<b>Description</b>	Buffer overflow in the X render (Xrender) extension in X.org X server 6.8.0 up to allows attackers to cause a denial of service

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.7.0	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.8	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.8.1	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.9	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.7.0	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.8	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.8.1	All	All	All
Application	<a href="#">X.org</a>	<a href="#">X11r6</a>	6.9	All	All	All

## References

Reference	Source	Link
Secunia - Advisories - Ubuntu update for xserver-xorg	SECUNIA	<a href="#">secu</a>
Repository / Oval Repository	OVAL	<a href="#">oval</a>
Security Announcement	SUSE	<a href="#">www</a>
Gentoo Linux Documentation -- X.Org: Buffer overflow in XRender extension	GENTOO	<a href="#">www</a>
USN-280-1: X.org server vulnerability   Ubuntu security notices	UBUNTU	<a href="#">usn.</a>
Mandriva update for xorg-x11 - Advisories - Secunia	SECUNIA	<a href="#">secu</a>

Advisories - Mandriva Linux	MANDRIVA	<a href="#">www</a>
Secunia - Advisories - SUSE update for xorg-x11-server	SECUNIA	<a href="#">secu</a>
OpenBSD update for x.org - Advisories - Secunia	SECUNIA	<a href="#">secu</a>
Secunia - Advisories - X.Org X11 Render Extension Buffer Overflow Vulnerability	SECUNIA	<a href="#">secu</a>
OpenBSD 3.8 errata	OPENBSD	<a href="#">www</a>
SecurityFocus	FEDORA	<a href="#">www</a>
Sun Solaris update for Xorg X Server - Advisories - Secunia	SECUNIA	<a href="#">secu</a>
IBM X-Force Exchange	XF	<a href="#">exch</a>
US-CERT Vulnerability Note VU#633257	CERT-VN	<a href="#">www</a>
X.Org XRender Extension Buffer Overflow Vulnerability	BID	<a href="#">www</a>
Webmail - OVH	VUPEN	<a href="#">www</a>
SecurityTracker.com Archives - X Server Buffer Overflow Render Extension Lets Remote Users Execute Arbitrary Code	SECTRACK	<a href="#">secu</a>
2006-0024	TRUSTIX	<a href="#">www</a>
Gentoo update for xorg-x11 - Advisories - Secunia	SECUNIA	<a href="#">secu</a>
[CVE-2006-1525] X.Org security advisory: Buffer overflow in the Xrender extension	MLIST	<a href="#">lists.</a>
Bug 6642 – XCB rendertest crashes server	CONFIRM	<a href="#">bugs</a>
#102339: Security Vulnerability in the Xorg(1) Version of the Render Extension	SUNALERT	<a href="#">suns</a>
Support	REDHAT	<a href="#">www</a>
Red Hat update for xorg-x11 - Advisories - Secunia	SECUNIA	<a href="#">secu</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd.</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)