



CVE-2006-6101

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2006-6101
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-31 05:00:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	Integer overflow in the ProcRenderAddGlyphs function in the Render extension for X.Org 6.8.2, 6.9.0, 7.0, and 7.1, and XF

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	X.org	X.org	6.8.2	All	All	All
Application	X.org	X.org	6.9.0	All	All	All
Application	X.org	X.org	7.0	All	All	All
Application	X.org	X.org	7.1	All	All	All
Application	X.org	X.org	6.8.2	All	All	All
Application	X.org	X.org	6.9.0	All	All	All
Application	X.org	X.org	7.0	All	All	All
Application	X.org	X.org	7.1	All	All	All
Application	Xfree86 Project	Xfree86	All	All	All	All
Application	Xfree86 Project	Xfree86	All	All	All	All

References

Reference	Source	Link
ASA-2007-066 (RHSA-2007-0002)	CONFIRM	supp
Security Announcement	SUSE	www
rhn.redhat.com Red Hat Support	REDHAT	www
Gentoo Linux Documentation -- X.Org X server: Multiple vulnerabilities	GENTOO	secu

HP-UX update for Xserver - Advisories - Secunia	SECUNIA	secu
Repository / Oval Repository	OVAL	oval
Webmail - OVH	VUPEN	www
XFree86 "DBE" and "Render" Extensions Vulnerabilities - Advisories - Secunia	SECUNIA	secu
Ubuntu update for xserver-xorg-core - Advisories - Secunia	SECUNIA	secu
Gentoo update for xorg-server - Advisories - Secunia	SECUNIA	secu
SUSE update for XFree86 and Xorg - Advisories - Secunia	SECUNIA	secu
Webmail - OVH	VUPEN	www
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	slack
Debian update for xfree86 - Advisories - Secunia	SECUNIA	secu
Red Hat update for xorg-x11 - Advisories - Secunia	SECUNIA	secu
20070109 Multiple Vendor X Server Render Extension ProcRenderAddGlyphs Memory Corruption Vulnerability	IDEFENSE	labs
ASA-2007-074 (SUN 102803)	CONFIRM	supp
32084	OSVDB	osvc
Webmail - OVH	VUPEN	www
Avaya CMS xfs / X Render and DBE Extensions Vulnerabilities - Advisories - Secunia	SECUNIA	secu
Advisories - Mandriva Linux	MANDRIVA	www
X.Org X11 "DBE" and "Render" Extensions Vulnerabilities - Advisories - Secunia	SECUNIA	secu
IBM X-Force Exchange	XF	exch
Avaya Products XFree86 "DBE" and "Render" Extensions Vulnerabilities - Advisories - Secunia	SECUNIA	secu
Mandriva update for xorg-x11 - Advisories - Secunia	SECUNIA	secu
[ANNOUNCE] X.Org Security Advisory: multiple integer overflows in dbe and render extensions	MLIST	lists
SSRT071295	HP	h200
Webmail - OVH	VUPEN	www
X.Org DBE And Render Extensions Multiple Local Integer Overflow Vulnerabilities	BID	www
Webmail - OVH	VUPEN	www
issues.rpath.com/browse/RPL-920	CONFIRM	issu
Support	REDHAT	www
Sun Solaris X Font Server / X Render and DBE Extensions Vulnerabilities - Advisories - Secunia	SECUNIA	secu
Slackware update for x11 - Secunia.com	SECUNIA	secu
NetBSD-SA2007-002	NETBSD	ftp.n
USN-403-1: X.org vulnerabilities Ubuntu	UBUNTU	www
rPath update for xorg-x11 - Advisories - Secunia	SECUNIA	secu
Debian -- Security Information -- DSA-1249-1 xfree86	DEBIAN	www
X Memory Corruption Errors in Render and DBE Extensions Let Local Users Gain Root Privileges - SecurityTracker	SECTRACK	secu
"40000 Multiple Vendor X Server Render Extension ProcRenderAddGlyphs Memory Corruption Vulnerability"	CONFIRM	

#102803: Multiple Integer Overflow Vulnerabilities in the X Font Server (xfs(1)) and the X Render and DBE Extensions	SUNALERT	SUN
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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](#)