CVE-2008-2361

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-2361
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-16 19:41:00 UTC
Updated	2018-10-11 20:40:00 UTC
Description	Integer overflow in the ProcRenderCreateCursor function in the Render extension in the X server 1.4 in X.Org X11R7.3 allo

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xorg	X11	r7.3	All	All	All
Application	Xorg	X11	r7.3	All	All	All

References

Reference
SecurityFocus
APPLE-SA-2009-02-12 Security Update 2009-001
Debian update for xorg-server - Secunia Advisories - Vulnerability Intelligence - Secunia.com
ASA-2008-249 (SUN 238686)
rhn.redhat.com | Red Hat Support
USN-616-1: X.org vulnerabilities | Ubuntu
Support
OpenBSD update for X.Org - Secunia Advisories - Vulnerability Intelligence - Secunia.com
rPath update for xorg-x11 - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Debian update for xorg-server - Secunia Advisories - Vulnerability Intelligence - Secunia.com
SUSE update for xorg-x11 and XFree86 - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Repository / Oval Repository

Support / Security / Advisories / / MDVSA-2008:179 | Mandriva

Gentoo update for xorg-server - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Gentoo update for nx - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

ftp.freedesktop.org/pub/xorg/X11R7.3/patches/xorg-xserver-1.4-cve-2008-2361.diff

X.Org X server: Multiple vulnerabilities — Gentoo Linux Documentation

Sun Solaris X Server Extensions Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

issues.rpath.com/browse/RPL-2619

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

20080611 Multiple Vendor X Server Render Extension ProcRenderCreateCursor() Integer Overflow Vulnerability

Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

SecurityFocus

X.Org X Server RENDER Extension 'ProcRenderCreateCursor()' Denial of Service Vulnerability

Avaya CMS / IR Solaris X Server Extensions Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Red Hat update for xorg-x11-server - Secunia Advisories - Vulnerability Intelligence - Secunia.com

wiki.rpath.com/wiki/Advisories:rPSA-2008-0201

Red Hat update for XFree86 - Secunia Advisories - Vulnerability Intelligence - Secunia.com

issues.rpath.com/browse/RPL-2607

button->down used inconsistently

Support / Security / Advisories / / MDVSA-2008:115 | Mandriva

Ubuntu update for xorg-server - Secunia Advisories - Vulnerability Intelligence - Secunia.com

NX: User-assisted execution of arbitrary code — Gentoo Linux Documentation

Support / Security / Advisories / / MDVSA-2008:116 | Mandriva

Debian -- Security Information -- DSA-1595-1 xorg-server

SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com

[security-announce] SUSE Security Announcement: X.org/XFree86 security p

[security-announce] SUSE Security Summary Report: SUSE-SR:2008:019

rhn.redhat.com | Red Hat Support

X.org X11 Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

About the security content of Security Update 2009-001

SecurityTracker.com Archives - X Integer Overflow in ProcRenderCreateCursor() Lets Local Users and Remote Authenticated Users Execute

#238686: Multiple Security Vulnerabilities in the Solaris X Server Extensions may lead to a Denial of Service (DoS) condition or allow Executic

Fedora update for xorg-x11-server - Secunia Advisories - Vulnerability Intelligence - Secunia.com

CVE Program record

NVD vulnerability detail

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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