



CVE-2006-3740

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-3740
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-13 01:07:00 UTC
Updated	2018-10-17 21:29:00 UTC
Description	Integer overflow in the scan_cidfont function in X.Org 6.8.2 and XFree86 X server allows local users to execute arbitrary co

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	6.8.2	All	All	All
Application	Xfree86 Project	Xfree86 X	All	All	All	All
Application	Xfree86 Project	Xfree86 X	All	All	All	All

References

Reference	Source
Webmail - OVH	VULN
usn/usn-344-1 - Ubuntu: Linux for human beings	UBUNTU
VMware ESX Server 2.5.4 Upgrade Patch 5 (for 2.5.4 Systems Only)	CONFIRMED
X11 libXfont CID Encoded Fonts Integer Overflows - Advisories - Secunia	SECUNIA
Mandriva update for xorg-x11 - Advisories - Secunia	SECUNIA
#102780: Two Integer Overflow Vulnerabilities Found in the Xorg(1) X Server	SUSE
X.Org LibXfont CID Font File Multiple Integer Overflow Vulnerabilities	BID
Advisories - Mandriva Linux	MANDRIVA
Avaya Modular Messaging X11 libXfont Integer Overflows - Advisories - Secunia	SECUNIA
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA

Accenture Let there be change	IDE
Ubuntu updates for libxfont / xorg - Advisories - Secunia	SEC
Red Hat update for XFree86 - Advisories - Secunia	SEC
IBM X-Force Exchange	XF
Security Announcement	SUS
SecurityFocus	BUK
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUI
rhn.redhat.com Red Hat Support	REI
[#RPL-614] local root privilege escalation vulnerabilities in CID fonts parser: CVE-2006-3739 CVE-2006-3740 - rPath JIRA	CO
rPath update for xorg-x11 - Advisories - Secunia	SEC
Red Hat update for xorg-x11 - Advisories - Secunia	SEC
XFree86 CID Encoded Fonts Integer Overflows - Advisories - Secunia	SEC
SecurityFocus	BUK
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUI
Repository / Oval Repository	OV,
Gentoo Linux Documentation -- LibXfont, monolithic X.org: Multiple integer overflows	GEI
Debian update for xfree86 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
Debian -- Security Information -- DSA-1193-1 xfree86	DEI
Sun Solaris 10 Xorg X Server Integer Overflows - Advisories - Secunia	SEC
ASA-2006-190 (RHSA-2006-0665)	CO
Support	REI
Sun Solaris 9 Xorg X Server Integer Overflows - Advisories - Secunia	SEC
VMware ESX Server Multiple Security Updates - Advisories - Secunia	SEC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUI
Mandriva update for xorg-x11 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
SecurityTracker.com Archives - X Buffer Overflow in Processing CID-encoded Type1 Fonts Lets Remote Users Execute Arbitrary Code	SEC
Gentoo update for libXfont - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
ASA-2006-191 (RHSA-2006-0666)	CO
Avaya Products XFree86 Integer Overflow Vulnerabilities - Advisories - Secunia	SEC
CVE Program record	CVI
NVD vulnerability detail	NVI

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](#)