



CVE-2007-1352

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

Summary

CVE	CVE-2007-1352
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-06 01:19:00 UTC
Updated	2018-10-16 16:38:00 UTC
Description	Integer overflow in the FontFileInitTable function in X.Org libXfont before 20070403 allows remote authenticated users to e

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	9.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.1	All	ppc	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	2007	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	9.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.1	All	ppc	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All	All

Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	3.0	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux Corporate Server	4.0	All	x86_64	All
Application	Mandrakesoft	Mandrake Multi Network Firewall	2.0	All	All	All
Application	Mandrakesoft	Mandrake Multi Network Firewall	2.0	All	All	All
Operating System	Openbsd	Openbsd	3.9	All	All	All
Operating System	Openbsd	Openbsd	4.0	All	All	All
Operating System	Openbsd	Openbsd	3.9	All	All	All
Operating System	Openbsd	Openbsd	4.0	All	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All

Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	client	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	client_workstation	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	client	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	client_workstation	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Operating System	Redhat	Linux	9.0	All	i386	All
Operating System	Redhat	Linux	9.0	All	i386	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium	All
Operating System	Rpath	Linux	1	All	All	All
Operating System	Rpath	Linux	1	All	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All	All
Operating System	Slackware	Slackware Linux	current	All	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All	All
Operating System	Slackware	Slackware Linux	current	All	All	All
Operating System	Turbolinux	Turbolinux Desktop	10.0	All	All	All
Operating System	Turbolinux	Turbolinux Desktop	10.0	All	All	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia32	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	sparc	All

Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia32	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	5.10	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	sparc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	sparc	All
Application	X.org	Libxfont	1.2.2	All	All	All
Application	X.org	Libxfont	1.2.2	All	All	All

References

Reference

[rhn.redhat.com | Red Hat Support](#)

[APPLE-SA-2007-11-14 Safari 3 Beta Update 3.0.4 \(Windows\)](#)

[Webmail | OVH- OVH](#)

[IBM X-Force Exchange](#)

[OpenBSD 4.0 errata](#)

[USN-448-1: X.org vulnerabilities | Ubuntu](#)

[APPLE-SA-2009-02-12 Security Update 2009-001](#)

[OpenBSD 3.9 errata](#)

Debian -- Security Information -- DSA-1294-1 xfree86
Sun Solaris X11 Multiple Vulnerabilities - Advisories - Secunia
ImageMagick XGetPixel/XInitImage Multiple Integer Overflow Vulnerabilities
Ubuntu update for freetype, libxfont, xorg, and xorg-server - Advisories - Secunia
Gentoo Linux Documentation -- LibXfont, TightVNC: Multiple vulnerabilities
[ANNOUNCE] various integer overflow vulnerabilites in xserver, libX11 and libXfont
Red Hat update for XFree86 - Advisories - Secunia
X.Org LibXFont Multiple Local Integer Overflow Vulnerabilities
Webmail OVH- OVH
Support
Debian update for xfree86 - Secunia Advisories - Vulnerability Intelligence - Secunia.com
issues.foresightlinux.org/browse/FL-223
Security Announcement
20070403 Multiple Vendor X Server fonts.dir File Parsing Integer Overflow Vulnerability
Mandriva update for xorg-x11 - Secunia Advisories - Vulnerability Intelligence - Secunia.com
SecurityFocus
Support / Security / Advisories // MDKSA-2007:079 Mandriva
issues.rpath.com/browse/RPL-1213
Support / Security / Advisories // MDKSA-2007:080 Mandriva
rhn.redhat.com Red Hat Support
SecurityFocus
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
ASA-2007-178 (SUN 102886)
Repository / Oval Repository
X.Org X11 Multiple Vulnerabilities - Advisories - Secunia
XFree86 Multiple Vulnerabilities - Advisories - Secunia
SUSE update for XFree86 and Xorg - Advisories - Secunia
#102886: Multiple vulnerabilities in libfreetype, Xsun(1) and Xorg(1)
Mandriva update for tightvnc - Advisories - Secunia
Gentoo update for libXfont and tightvnc - Advisories - Secunia
Red Hat update for xorg-x11 - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Repository / Oval Repository
OpenBSD update for X.Org - Advisories - Secunia
rPath update for freetype, xorg-x11, xorg-x11-fonts, xorg-x11-tools, and xorg-x11-xfs - Secunia Advisories - Vulnerability Intelligence - Secunia.com
About the security content of Security Update 2009-001
Apple OS X / X.Org X11 Multiple Vulnerabilities - Advisories - Secunia

SecurityTracker.com Archives - X11 Overflows Let Local Users Gain Root Privileges

CVE Program record

NVD vulnerability detail



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](#)