



# CVE-2007-5760

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

## Summary

<b>CVE</b>	CVE-2007-5760
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-01-18 23:00:00 UTC
<b>Updated</b>	2018-10-15 21:46:00 UTC
<b>Description</b>	Array index error in the XFree86-Misc extension in X.Org Xserver before 1.4.1 allows context-dependent attackers to execu

## 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="#">Xserver</a>	All	All	All	All
Application	<a href="#">Xfree86 Project</a>	<a href="#">Xfree86-misc</a>	All	All	All	All
Application	<a href="#">Xfree86 Project</a>	<a href="#">Xfree86-misc</a>	All	All	All	All

## References

### Reference

- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- Repository / Oval Repository
- [SECURITY] Fedora 8 Update: xorg-x11-server-1.3.0.0-39.fc8
- Advisories | Mandriva
- Avaya CMS Solaris X Window System and X Server Multiple Vulnerabilities - Advisories - Secunia
- Advisories | Mandriva
- OpenBSD 4.2 errata
- SUSE update for Xorg and XFree - Secunia Advisories - Vulnerability Intelligence - Secunia.com
- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- X.Org X Server 'PassMessage' Request Local Privilege Escalation Vulnerability
- X.Org X server and Xfont library: Multiple vulnerabilities — Gentoo Linux Documentation

IBM X-Force Exchange
Webmail   OVH- OVH
SecurityFocus
Gentoo Bug 204362 - x11-base/xorg-server x11-libs/libXfont Multiple vulnerabilities (CVE-2007-{5760,5958,6427,6428,6429}CVE-2008-0006)
20080117 Multiple Vendor X Server XFree86-Misc Extension Invalid Array Index Vulnerability
[SECURITY] Fedora 7 Update: xorg-x11-server-1.3.0.0-15.fc7
ASA-2008-039 (SUN 103200)
Support
#200153: Multiple Security Vulnerabilities in the Solaris X Server Extensions May Lead to a Denial of Service (DoS) Condition or Allow Execut
ASA-2008-078 (SUN 200153, Previous, ID:, 103200)
Mandriva update for x11-server-xgl - Advisories - Secunia
Ubuntu update for libxfont and xorg-server - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Gentoo update for xorg-server and libxfont - Advisories - Secunia
Linux Terminal Server Project: Multiple vulnerabilities — Gentoo Linux Documentation
X.org X11 Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Mandriva update for x11-server - Advisories - Secunia
NX: User-assisted execution of arbitrary code — Gentoo Linux Documentation
Sun Solaris X Window System and X Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
RETIRED: X.Org X Server Local Privilege Escalation and Information Disclosure Vulnerabilities
rPath update for xorg-x11 - Advisories - Secunia
modular -> monolithic
OpenBSD update for X.Org - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Fedora update for xorg-x11-server - Advisories - Secunia
rhn.redhat.com   Red Hat Support
Advisories   Mandriva
Red Hat update for xorg-x11-server - Advisories - Secunia
OpenBSD 4.1 errata
[security-announce] SUSE Security Announcement: Xorg and XFree (SUSE-SA:
Debian update for xorg-server - Advisories - Secunia
issues.rpath.com/browse/RPL-2010
200153
NX Server X11 Multiple Vulnerabilities - Advisories - Secunia
Gentoo Itsp Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Debian -- Security Information -- DSA-1466-1 xorg-server
Red Hat update for xorg-x11 - Advisories - Secunia

X Server Bugs in XFree86, Xinput, LOG-CUP, MIT-SHM, and EVI Extensions Let Local Users Gain Root Privileges - Security Tracker

Gentoo update for nxnode and nx - Advisories - Secunia

Avaya CMS Sun Solaris X Window System and X Server Vulnerabilities - Advisories - Secunia

USN-571-1: X.org vulnerabilities | Ubuntu security notices

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](#)**