



CVE-2000-0976

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

Summary

CVE	CVE-2000-0976
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-12-19 05:00:00 UTC
Updated	2008-09-05 20:22:00 UTC
Description	Buffer overflow in xlib in XFree 3.3.x possibly allows local users to execute arbitrary commands via a long DISPLAY environ

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xfree86 Project	Xlib	3.3x	All	All	All
Application	Xfree86 Project	Xlib	3.3x	All	All	All

References

Reference	Source	Link
20001012 another Xlib buffer overflow	BUGTRAQ	archives.neohapsis.com
ISS X-Force Database: xfree-xlib-bo (5751): Xfree xlib buffer overflow allows arbitrary command execution	XF	www.iss.net
504 Gateway Time-out	BID	www.securityfocus.com
20020502-01-I	SGI	patches.sgi.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)