



CVE-2001-0955

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

Summary

CVE	CVE-2001-0955
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-09-22 04:00:00 UTC
Updated	2017-12-19 02:29:00 UTC
Description	Buffer overflow in fbglyph.c in XFree86 before 4.2.0, related to glyph clipping for large origins, allows attackers to cause a d

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	X11r6	4.0	All	All	All
Application	Xfree86 Project	X11r6	4.0.1	All	All	All
Application	Xfree86 Project	X11r6	4.0.3	All	All	All
Application	Xfree86 Project	X11r6	4.0	All	All	All
Application	Xfree86 Project	X11r6	4.0.1	All	All	All
Application	Xfree86 Project	X11r6	4.0.3	All	All	All

References

Reference	Source	Link	Tags
XFree86 fbglyph Denial of Service Vulnerability	BID	www.securityfocus.com	Patch, Vendor Advisory
CVS log for xc/programs/Xserver/fb/fbglyph.c	MISC	cvsweb.xfree86.org	
'Re: Crashing X' - MARC	BUGTRAQ	marc.info	
XTerm Title Bar Buffer Overflow Vulnerability	BID	www.securityfocus.com	Vendor Advisory
XFree86(TM): Security Issues	CONFIRM	www.xfree86.org	
'XFree86 DOS / Buffer overflow local and remote.' - MARC	VULN-DEV	marc.info	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	

'Crashing X' - MARC	BUGTRAQ	marc.info	
Summary of new features in 4.2.0.	CONFIRM	www.xfree86.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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