



CVE-2022-44617

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

Summary

CVE	CVE-2022-44617
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-06 23:15:00 UTC
Updated	2023-11-07 03:54:00 UTC
Description	A flaw was found in libXpm. When processing a file with width of 0 and a very large height, some parser functions will be ca

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libxpm Project	Libxpm	All	All	All	All
Application	X.org	Libxpm	All	All	All	All

References

Reference	Source	Li
[SECURITY] [DLA 3459-1] libxpm security update	MLIST	list
X.Org Security Advisory: Issues handling XPM files in libXpm prior to 3.5.15	MISC	list
2160193 – (CVE-2022-44617) CVE-2022-44617 libXpm: Runaway loop on width of 0 and enormous height	MISC	bu
Issues handling XPM files in libXpm prior to 3.5.15 (19) · Merge requests · xorg / lib / libXpm · GitLab	MISC	git
Fix CVE-2022-44617: Runaway loop with width of 0 and enormous height (f80fa6ae) · Commits · xorg / lib / libXpm · GitLab	MISC	git
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160419](#) Oracle Enterprise Linux Security Update for libxpm (ELSA-2023-0383)

160427 Oracle Enterprise Linux Security Update for libxpm (ELSA-2023-0379)
183631 Debian Security Update for libxpm (CVE-2022-44617)
199109 Ubuntu Security Notification for libXpm Vulnerabilities (USN-5807-1)
199563 Ubuntu Security Notification for libXpm Vulnerabilities (USN-5807-2)
241108 Red Hat Update for libxpm (RHSA-2023:0382)
241109 Red Hat Update for libxpm (RHSA-2023:0383)
241114 Red Hat Update for libxpm (RHSA-2023:0381)
241116 Red Hat Update for libxpm (RHSA-2023:0379)
241118 Red Hat Update for libxpm (RHSA-2023:0378)
241598 Red Hat Update for libxpm (RHSA-2023:0384)
241648 Red Hat Update for libxpm (RHSA-2023:0380)
283624 Fedora Security Update for libXpm (FEDORA-2023-1bd07375a7)
283635 Fedora Security Update for libXpm (FEDORA-2023-49dbeb6b03)
296099 Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)
354753 Amazon Linux Security Advisory for libXpm : ALAS-2023-1693
354782 Amazon Linux Security Advisory for libXpm : ALAS2-2023-1962
355068 Amazon Linux Security Advisory for libXpm : AL2012-2023-392
355197 Amazon Linux Security Advisory for libXpm : ALAS2023-2023-107
377954 Alibaba Cloud Linux Security Update for libxpm (ALINUX3-SA-2023:0011)
502637 Alpine Linux Security Update for libxpm
504114 Alpine Linux Security Update for libxpm
6000030 Debian Security Update for libxpm (DLA 3459-1)
672739 EulerOS Security Update for libxpm (EulerOS-SA-2023-1475)
672742 EulerOS Security Update for libxpm (EulerOS-SA-2023-1450)
672794 EulerOS Security Update for libxpm (EulerOS-SA-2023-1556)
672816 EulerOS Security Update for libxpm (EulerOS-SA-2023-1531)
672863 EulerOS Security Update for libxpm (EulerOS-SA-2023-1615)
672927 EulerOS Security Update for libxpm (EulerOS-SA-2023-1762)

672939 EulerOS Security Update for libxpm (EulerOS-SA-2023-1784)
673059 EulerOS Security Update for libxpm (EulerOS-SA-2023-2158)
691091 Free Berkeley Software Distribution (FreeBSD) Security Update for libxpm (38f213b6-8f3d-4067-91ef-bf14de7ba518)
753577 SUSE Enterprise Linux Security Update for libXpm (SUSE-SU-2023:0171-1)
753580 SUSE Enterprise Linux Security Update for libXpm (SUSE-SU-2023:0165-1)
905395 Common Base Linux Mariner (CBL-Mariner) Security Update for libXpm (13230)
907573 Common Base Linux Mariner (CBL-Mariner) Security Update for libXpm (13230-1)
940888 AlmaLinux Security Update for libXpm (ALSA-2023:0379)
940902 AlmaLinux Security Update for libXpm (ALSA-2023:0383)
960502 Rocky Linux Security Update for libXpm (RLSA-2023:0379)
960631 Rocky Linux Security Update for libXpm (RLSA-2023:0383)

© [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](#)