



CVE-2023-43789

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

Summary

CVE	CVE-2023-43789
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-12 12:15:00 UTC
Updated	2023-12-06 03:15:00 UTC
Description	A vulnerability was found in libXpm where a vulnerability exists due to a boundary condition, a local user can trigger an out-

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Libxpm Project	Libxpm	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 39 Update: libXpm-3.5.17-1.fc39 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproje
2242249 – (CVE-2023-43789) CVE-2023-43789 libXpm: out of bounds read on XPM with corrupted colormap	MISC	bugzilla.redhat.c
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...		lists.fedoraproje
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...		lists.fedoraproje
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...		lists.fedoraproje
cve-details	MISC	access.redhat.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199797](#) Ubuntu Security Notification for libXpm Vulnerabilities (USN-6408-1)

[199853](#) Ubuntu Security Notification for libXpm Vulnerabilities (USN-6408-2)

[284793](#) Fedora Security Update for motif (FEDORA-2023-25329c196b)

[284796](#) Fedora Security Update for motif (FEDORA-2023-ba2e60e743)

[285125](#) Fedora Security Update for motif (FEDORA-2023-e1c7fae02e)

[285221](#) Fedora Security Update for libXpm (FEDORA-2023-c4cf6646b9)

[296108](#) Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)

[356444](#) Amazon Linux Security Advisory for libXpm : ALAS2-2023-2295

[356525](#) Amazon Linux Security Advisory for libXpm : ALAS2023-2023-382

[356545](#) Amazon Linux Security Advisory for libXpm : ALAS-2023-1875

[356987](#) Amazon Linux Security Advisory for libXpm : AL2012-2023-471

[505892](#) Alpine Linux Security Update for libxpm

[6000113](#) Debian Security Update for libxpm (DLA 3603-1)

[6000189](#) Debian Security Update for libxpm (DSA 5516-1)

[673475](#) EulerOS Security Update for libxpm (EulerOS-SA-2023-3312)

[673610](#) EulerOS Security Update for libxpm (EulerOS-SA-2024-1091)

[673729](#) EulerOS Security Update for libxpm (EulerOS-SA-2023-3344)

[673776](#) EulerOS Security Update for libxpm (EulerOS-SA-2024-1067)

[673837](#) EulerOS Security Update for libxpm (EulerOS-SA-2023-3279)

[673922](#) EulerOS Security Update for libxpm (EulerOS-SA-2024-1151)

[674060](#) EulerOS Security Update for libxpm (EulerOS-SA-2023-3251)

[691326](#) Free Berkeley Software Distribution (FreeBSD) Security Update for x11/libxpm Multiple Vulnerabilities (199cdb4d-690d-11ee-9ed0-001fc69cd6dc)

[755027](#) SUSE Enterprise Linux Security Update for libXpm (SUSE-SU-2023:3965-1)

[755029](#) SUSE Enterprise Linux Security Update for libXpm (SUSE-SU-2023:3962-1)

[907596](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libXpm (31490-1)

© [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](#)