



CVE-2023-43786

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

Summary

CVE	CVE-2023-43786
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-10 13:15:00 UTC
Updated	2024-01-24 21:15:00 UTC
Description	A vulnerability was found in libX11 due to an infinite loop within the PutSubImage() function. This flaw allows a local user to

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	X.org	Libx11	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 39 Update: libXpm-3.5.17-1.fc39 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
cve-details	MISC	access.redhat.com
October 2023 libX11 Vulnerabilities in NetApp Products NetApp Product Security	MISC	security.netapp.com
oss-security - Re: Fwd: X.Org Security Advisory: Issues in libX11 prior to 1.8.7 & libXpm prior to 3.5.17		www.openwall.com
2242253 – (CVE-2023-43786) CVE-2023-43786 libX11: stack exhaustion from infinite recursion in PutSubImage()	MISC	bugzilla.redhat.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.

Legacy QID Mappings

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

[199800](#) Ubuntu Security Notification for libx11 Vulnerabilities (USN-6407-1)

[199821](#) Ubuntu Security Notification for libx11 Vulnerabilities (USN-6407-2)

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

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

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

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

[356542](#) Amazon Linux Security Advisory for libX11 : ALAS2023-2023-383

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

[356774](#) Amazon Linux Security Advisory for libX11 : ALAS2-2023-2356

[356779](#) Amazon Linux Security Advisory for libX11 : ALAS-2023-1895

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

[356997](#) Amazon Linux Security Advisory for libX11 : AL2012-2023-481

[503467](#) Alpine Linux Security Update for libx11

[505891](#) Alpine Linux Security Update for libx11

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

[6000133](#) Debian Security Update for libx11 (DLA 3602-1)

[6000211](#) Debian Security Update for libx11 (DSA 5517-1)

[673510](#) EulerOS Security Update for libx11 (EulerOS-SA-2023-3249)

[673631](#) EulerOS Security Update for libxpm (EulerOS-SA-2024-1282)

[673653](#) EulerOS Security Update for libx11 (EulerOS-SA-2024-1150)

[673658](#) EulerOS Security Update for libx11 (EulerOS-SA-2024-1281)

[673663](#) EulerOS Security Update for libxpm (EulerOS-SA-2024-1340)

[673682](#) EulerOS Security Update for libx11 (EulerOS-SA-2024-1089)

[673699](#) EulerOS Security Update for libx11 (EulerOS-SA-2023-3310)

[673702](#) EulerOS Security Update for libxpm (EulerOS-SA-2024-1318)

[673769](#) EulerOS Security Update for libxpm (EulerOS-SA-2024-1180)

[673940](#) EulerOS Security Update for libx11 (EulerOS-SA-2023-3277)

673977 EulerOS Security Update for libxpm (EulerOS-SA-2024-1200)
674022 EulerOS Security Update for libx11 (EulerOS-SA-2023-3342)
674040 EulerOS Security Update for libx11 (EulerOS-SA-2024-1065)
691325 Free Berkeley Software Distribution (FreeBSD) Security Update for 11/libx11 Multiple Vulnerabilities (bd92f1ab-690c-11ee-9ed0-001fc69cd6dc)
755028 SUSE Enterprise Linux Security Update for libX11 (SUSE-SU-2023:3963-1)
755044 SUSE Enterprise Linux Security Update for libX11 (SUSE-SU-2023:3989-1)
907588 Common Base Linux Mariner (CBL-Mariner) Security Update for libX11 (31321-1)

© [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](#)