



CVE-2019-9959

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

Summary

CVE	CVE-2019-9959
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-22 15:15:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	The JPXStream::init function in Poppler 0.78.0 and earlier doesn't check for negative values of stream length, leading to an

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Freedesktop	Poppler	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 29 Update: poppler-0.67.0-22.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 1963-1] poppler security update	MLIST	lists.debian.org
[SECURITY] Fedora 30 Update: poppler-0.73.0-14.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Poppler CVE-2019-9959 Integer Overflow Vulnerability	BID	www.securityfocus.com
[SECURITY] Fedora 29 Update: poppler-0.67.0-22.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 30 Update: poppler-0.73.0-14.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
NEWS · master · poppler / poppler · GitLab	CONFIRM	gitlab.freedesktop.org
[SECURITY] [DLA 3120-1] poppler security update	MLIST	lists.debian.org
[SECURITY] [DLA 2440-1] poppler security update	MLIST	lists.debian.org
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

- [181075](#) Debian Security Update for poppler (DLA 3120-1)
- [377260](#) Alibaba Cloud Linux Security Update for poppler and evince (ALINUX2-SA-2020:0052)
- [500528](#) Alpine Linux Security Update for poppler
- [504295](#) Alpine Linux Security Update for poppler
- [751420](#) SUSE Enterprise Linux Security Update for poppler (SUSE-SU-2021:3854-1)
- [751427](#) OpenSUSE Security Update for poppler (openSUSE-SU-2021:3854-1)
- [752145](#) SUSE Enterprise Linux Security Update for poppler (SUSE-SU-2022:1723-1)
- [752148](#) SUSE Enterprise Linux Security Update for poppler (SUSE-SU-2022:1724-1)

© 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](#).

