



# CVE-2018-20650

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

## Summary

<b>CVE</b>	CVE-2018-20650
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-01-01 16:29:00 UTC
<b>Updated</b>	2023-02-11 18:12:00 UTC
<b>Description</b>	A reachable Object::dictLookup assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to the lack of a

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Freedesktop</a>	<a href="#">Poppler</a>	0.72.0	All	All	All
Application	<a href="#">Freedesktop</a>	<a href="#">Poppler</a>	0.72.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="#">access.r</a>
USN-3865-1: poppler vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubun</a>
Poppler CVE-2018-20650 Denial of Service Vulnerability	BID	<a href="#">www.sec</a>
a reachable abort in FileSpec::FileSpec in FileSpec.cc (#704) · Issues · poppler / poppler · GitLab	MISC	<a href="#">gitlab.fre</a>
FileSpec: Move the fileSpec.dictLookup call inside fileSpec.isDict if (de0c0b83) · Commits · poppler / poppler · GitLab	MISC	<a href="#">gitlab.fre</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.r</a>
[SECURITY] [DLA 1939-1] poppler security update	MLIST	<a href="#">lists.debi</a>
[SECURITY] [DLA 3120-1] poppler security update	MLIST	<a href="#">lists.debi</a>
[SECURITY] [DLA 2440-1] poppler security update	MLIST	<a href="#">lists.debi</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[181075](#) Debian Security Update for poppler (DLA 3120-1)

[296089](#) Oracle Solaris 11.4 Support Repository Update (SRU) 10.1.3 Missing (CPUAPR2019)

[377321](#) Alibaba Cloud Linux Security Update for poppler (ALINUX2-SA-2019:0096)

[670666](#) EulerOS Security Update for poppler (EulerOS-SA-2021-2425)

[751420](#) SUSE Enterprise Linux Security Update for poppler (SUSE-SU-2021:3854-1)

[751427](#) OpenSUSE Security Update for poppler (openSUSE-SU-2021:3854-1)

[754197](#) SUSE Enterprise Linux Security Update for poppler (SUSE-SU-2023:2907-1)

[754198](#) SUSE Enterprise Linux Security Update for poppler (SUSE-SU-2023:2906-1)

© [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](#)