CVE-2019-9903

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-9903
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 18:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	PDFDoc::markObject in PDFDoc.cc in Poppler 0.74.0 mishandles dict marking, leading to stack consumption in the functior

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Freedesktop	Poppler	0.74.0	All	All	All
Application	Freedesktop	Poppler	0.74.0	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 28 Update: poppler-0.62.0-22.fc28 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 30 Update: poppler-0.73.0-8.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
stack-overflow in Dict::find() (#741) · Issues · poppler / poppler · GitLab	MISC	gitlab.freedesktop.org
CVE-2019-9903: Stack-based Buffer Overflows in Dict::find() - poppler 0.74.0 - Loginsoft Research	MISC	research.loginsoft.com
107560	BID	www.securityfocus.com
[SECURITY] Fedora 29 Update: poppler-0.67.0-18.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Red Hat Customer Portal	REDHAT	access.redhat.com
[SECURITY] Fedora 28 Update: poppler-0.62.0-22.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
USN-4042-1: poppler vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] Fedora 29 Update: poppler-0.67.0-18.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 30 Update: poppler-0.73.0-8.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] [DLA 3120-1] 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)
- 296089 Oracle Solaris 11.4 Support Repository Update (SRU) 10.1.3 Missing (CPUAPR2019)
- 670244 EulerOS Security Update for poppler (EulerOS-SA-2021-1832)
- 670666 EulerOS Security Update for poppler (EulerOS-SA-2021-2425)
- 670920 EulerOS Security Update for poppler (EulerOS-SA-2021-1832)
- 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)