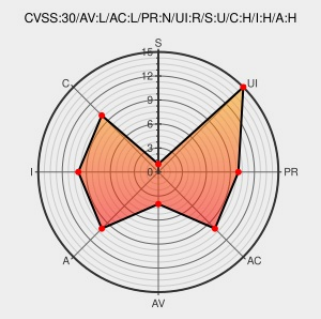
CVE-2015-8868

Published on: 05/06/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8868

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Heap-based buffer overflow in the ExponentialFunction::ExponentialFunction function in Poppler before 0.40.0 allows remote attackers to cause a denial of service (memory corruption and crash) or possibly execute arbitrary code via an invalid blend mode in the ExtGState dictionary in a crafted PDF document.

CVE-2015-8868 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2580

openSUSE-SU-2016:1630-1: moderate: Security update for poppler	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1630
[SECURITY] Fedora 23 Update: mingw-poppler-0.34.0-2.fc23	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-c848d48286
Debian -- Security Information -- DSA-3563-1 poppler	www.debian.org Depreciated Link text/html	DEBIAN DSA-3563
USN-2958-1: poppler vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2958-1
Poppler	poppler.freedesktop.org text/html	CONFIRM poppler.freedesktop.org/releases.html
openSUSE-SU-2016:1322-1: moderate: Security update for poppler	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1322
poppler/poppler - The poppler pdf rendering library (mirrored from https://gitlab.freedesktop.org/poppler/poppler)	cgit.freedesktop.org text/html	CONFIRM cgit.freedesktop.org/poppler/poppler/commit/?id=b3425dd3261679958cd56c0f71995c15d2124433
[SECURITY] Fedora 22 Update: mingw-poppler-0.30.0-4.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-3c4e438fc8
Poppler CVE-2015-8868 Heap Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 89324
oss-security - CVE request: Poppler < 0.40.0	www.openwall.com text/x-python	MLIST [oss-security] 20160411 CVE request: Poppler < 0.40.0
93476 – Memory Corruption while processing Blend Mode	bugs.freedesktop.org text/html	CONFIRM bugs.freedesktop.org/show_bug.cgi?id=93476
Poppler: Multiple vulnerabilities (GLSA 201611-15) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201611-15

Related QID Numbers

670304 EulerOS Security Update for compat-poppler022 (EulerOS-SA-2021-1772)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating	Canonical	Ubuntu Linux	14.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Freedesktop	Poppler	0.39.0	All	All	All
Application	Freedesktop	Poppler	0.39.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:a:freedesktop:poppler:0.39.0:*:*:*:*:*:*:*:

cpe:2.3:a:freedesktop:poppler:0.39.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→